IDS Modeling and Evaluation in WANETs against Black/Gray-hole Attacks using Stochastic Models

Reza Entezari-Maleki
School of Computer Science,
Institute for Research in Fundamental Sciences (IPM),
Tehran, Iran.
E-mail: entezari@ipm.ir

Mohammed Gharib
Department of Computer Engineering,
Sharif University of Technology,
Tehran, Iran.
E-mail: gharib@ce.sharif.edu

Maryam Khosravi
Department of Computer Engineering,
Sharif University of Technology,
Tehran, Iran.
E-mail: m.khosravi26@gmail.com

Ali Movaghar
Department of Computer Engineering,
Sharif University of Technology,
Tehran, Iran.
E-mail: movaghar@sharif.edu

Abstract: The aim of this paper is to model and evaluate the performance of intrusion detection systems (IDSs) facing black-hole and gray-hole attacks within wireless ad hoc networks (WANETs). The main performance metric of an IDS in a WANET can be defined as the mean time required for the IDS to detect an attack in the network. To evaluate this measure, two types of stochastic models called continuous time Markov chain (CTMC) and stochastic reward net (SRN) are used in this paper. In the first step, two different CTMCs are proposed to model the black-hole and gray-hole attacks, and then, the method of computing the mean time to attack detection is presented on the proposed CTMCs. Since the numbers of states of the proposed CTMCs grow rapidly with increasing the number of the intermediate nodes and the number of attacks which should be done by a single node to trigger the IDS to detect the attack, SRNs are exploited to automatically generate the proposed CTMCs in the second step. The proposed SRNs for the black-hole and gray-hole attacks can appropriately model the network and the process of sending and receiving the messages. Different scenarios are designed to evaluate and compare IDSs on WANETs which show the applicability and usefulness of the proposed CTMCs and SRNs in real networks.

Keywords: Intrusion detection system; black-hole attack; gray-hole attack; Markov chain; stochastic reward net.

1 Introduction

Wireless ad hoc networks (WANETs) have been attracting the attention of a large number of researchers in the last years since WANETs are structureless, cost effective, flexible and scalable networks [1, 2]. Nodes within WANETs are communicating with each other directly if they are in the communication range of each other; otherwise, intermediate nodes are used to establish a connection between the communicating nodes. Due to the structureless nature of WANETs, security problem is more challenging in such networks. Generally, security is known as a more challenging concern in different networks while it needs some services to be satisfied. The main security services in a network

Copyright © 2015 Inderscience Enterprises Ltd.

are availability, confidentiality, integrity, authentication and non-repudiation [3]. Cryptography is considered as a promising solution to help to meet such services, but unfortunately, it can not fully satisfy all requirements, specifically the availability which is very important requirement in wireless networks [4]. Power, memory and process limitations of nodes, mobility of nodes, and the need for cooperating nodes in WANETs make security solutions more challenging in such networks.

The main security lack within WANETs is that any adversary node can read the messages which are sent in its communication range due to the wireless nature of the network. Moreover, it can drop or even change any message which is routed by itself. Dropping all the messages in WANETs is named black-hole attack while it is done by an adversary intermediate node which pretends itself as a node on the optimal path between the source and destination nodes [5]. Hence, the path containing the adversary node is always chosen by the source node as the main path to send all messages to the destination. Furthermore, if the adversary node selectively drops the messages, the attack is called gray-hole attack. Such attack is more serious and also harder to detect in comparison with the black-hole attack [6]. Availability is a security service which is vulnerable against both the black-hole and gray-hole attacks. In order to detect such attacks, all nodes or some of them should be equipped with an intrusion detection system (IDS) [7, 8] to discover the adversary node, and isolate it from the network. Each node in a network is equipped with an IDS which is a hardware or software tool to monitor the network and activities of the nodes for malicious behaviors. Moreover, it may be used for detecting policy outrages and abnormal activities.

There are several metrics which could be used to evaluate the performance of an IDS. False positive and false negative rates, detection rate, precision rate, mean time to detect and mean time to repair are examples of such metrics [9, 10, 11]. Moreover, these metrics are combined with some typical performance metrics like throughput, goodput, cost and so forth to capture a complete evaluation of an IDS [12, 13]. Since we use stochastic models to evaluate the performance of an IDS, we use the mean time to detect as the main performance metric in our evaluations. It is a dependable and widespread metric which had been used to evaluate the performance measure in many recent research work [14, 15, 16]. The mean time to detect an attack by an IDS is a factor which can be used to analyze different IDSs and their sensitivities to the various parameters of the network. In this paper, continuous time Markov chains (CTMCs) [17, 18] and stochastic reward nets (SRNs) [19, 20] are used to model and evaluate IDSs within WANETs. To do this, in the first step, two CTMCs are proposed to model black-hole and gray-hole attacks in a WANET. The first proposed CTMC models a black-hole attack in a WANET which contains a single source node, a single destination node, and N intermediate nodes. The source node initiates a session to find a route between itself and the destination node by broadcasting a route request message. This message can be safely delivered by the destination node, which will be replied by a real route reply message, or attacked by one of the intermediate nodes which will be relied by a fake route reply message. The IDS is assumed to detect the black-hole attack in the network when m consecutive attacks have been seen from a single intermediate node. After modeling the black-hole attack by CTMCs, the method to compute mean time to absorption in the proposed CTMC is presented to reflect the mean time to attack detection in the network. The second CTMC models a gray-hole attack in which the attacker to the route request message may or may not attack other route request messages sent by the source node after the first attack. Modeling this type of attacks in WANETs is harder than the black-hole attacks because the number of the attacks and the attackers should be considered in each of the states of the Markov chain before being able to properly model the attack. The CTMC proposed for gray-hole attack is also an absorbing CTMC which can be used to compute the mean time to attack detection within the network.

In practice, drawing and analyzing the proposed CTMCs for a network with large number of intermediate nodes and attacks (big values of parameters N and m) are impossible, so we need an automatic way to generate and analyze these CTMCs. To fulfill this requirement, two different SRNs are presented to model the black-hole and gray-hole attacks in a simple way. The usefulness of the proposed SRNs is more exhibited in a gray-hole attack in which creating and solving its CTMC are almost impossible for large values of intermediate nodes and also more number of attacks. Moreover, analyzing the proposed SRNs and computing the mean time to attack detection and probability of occurring i attacks in a time instant are possible using SRN supported tools. This matter together with various scenarios which show the applicability of the models in computing some useful measures and analyzing different aspects of the networks using the proposed CTMCs and SRNs is shown in this paper after discussing the models with details.

The remainder of this paper is organized as follows. Section 2 introduces some related research done in the field of modeling IDSs and other security issues using various mathematical models. Moreover, some research papers which have used different extensions of Petri nets to model security aspects of the systems are introduced in Section 2. Section 3 provides a short overview on CTMCs and SRNs, and explains some basic concepts of these two modeling approaches. Section 4 defines the problem and gives a short description of the system under study and its related assumptions. In Sections 5 and 6, the proposed CTMCs and SRNs for modeling an IDS in WANETs considering black-hole and gray-hole attacks are presented, respectively. In Section 7 detailed examples together with numerical results for various scenarios are provided. Finally, Section 8 concludes the paper and presents some guidelines for future work.

2 Related Work

Intrusion detection systems are divided into two general categories. The first category includes those IDSs which are designed to detect a single type of attacks. The second category contains the IDSs that can deal with a range of attacks. As an example of the first category, Medadian et al. [21] have proposed a black-hole detection method for ad-hoc on-demand distance vector (AODV). In this method, the receiver node, on receiving a reply, initiates a judgment process about the replier. A decision is made based on the opinions of the neighbors which are shared about the replier. Zhang et al. [22] have proposed a black-hole detection scheme based on sequence number checking of the route request (RREP) packets. Xiaopeng et al. [23] have proposed a gray-hole detection scheme for the dynamic source routing (DSR) protocol. This requires each node to produce evidence on forwarding packets using an aggregated signature algorithm. Another mechanism for gray hole detection in AODV have proposed in [24], which requires all nodes to maintain their neighbors data forwarding information.

As the recent research work proposed in the second category, we can refer the work done by Mitrokotsa et al. [25] where an IDS for ad hoc networks has been proposed by exploiting neural network and watermarking techniques. They used self-organizing maps in conjunction with machine learning and watermarking techniques to design an IDS. Syntax and semantic based approaches have also been proposed for network based IDSs in fixed networks [26]. Chang et al. [27] have presented an IDS for MANETs at the application layer. Their IDS utilizes both anomaly and misuse detection schemes to identify attacks in such networks. Shengrong et al. in [28] formulated a partially observable Markov decision process (POMDP) multi-armed bandit problem to obtain the optimal scheme of combining continuous user authentication and IDSs in a distributed manner. Afterwards, they presented a structural results method to solve the problem for a large network with a variety of nodes. In [13], distributed combined authentication and intrusion detection with data fusion in high-security MANETs have been studied. Multi-modal biometrics are deployed to work with IDSs to alleviate the shortcomings of unimodal biometric systems. In [29], a distributed IDS based on timed automata was given, and a cluster-based detection scheme was presented where a node is periodically elected as the monitor node for a cluster.

There are some research papers focusing on modeling and evaluation of IDSs using analytical models such as Markov chains and various extensions of Petri nets. In the following, some of the papers which have been recently published in this research area are introduced.

Cho et al. [8] have proposed a mathematical model based on SPNs to analyze the effect of IDSs on failure time of mission-oriented group communication system (GCS). The mean time to security failure (MTTSF) as a metric to identify the optimal intrusion detection rate was assessed in [8]. The difficulty with the model presented in [8] is considering a linear function for the attacker which is not realistic behavior in real networks. The same authors were studied the impact of IDS on performance of mobile GCS using SPN models [30]. They identified the best detection interval to optimize MTTSF metric, and minimize the communication cost.

Huang et al. [31] have proposed HWMP routing protocol model based on colored Petri nets (CPNs) in a wireless mesh network (WMN). The proposed model can detect the existence of black-hole attacks. Furthermore, a security routing algorithm to prevent the black-hole attack to be happened was presented in [31], and then, the effectiveness of this mechanism was discussed. Dasgupta [32] have presented a CPN model to analyze an anti black-hole mechanism (ABM) for detecting a black-hole attack in MANET. Azgomi et al. [33] have proposed a CPN model for EQ-MAC protocol, an energy aware MAC protocol for wireless sensor network (WSN). The paper considers performance of EQ-MAC protocol, but does not perform model checking.

Sedaghatbaf et al. [34] have proposed a new attack modeling approach based on hierarchical and colored extension of stochastic activity networks (HCSANs) which can model the dynamic behavior of an attacker. This approach is useful for security measures estimation, including MTTSF and attack success probability (ASP). However, it only handles modeling a single attacker's behavior, and has not the ability to model coordinated attacks. Jayaparvathy et al. [35] and Younes et al. [36] have used SRNs to model the IEEE 802.11 DCF MAC protocol. In [35], the mean delay and the average system throughput of this protocol were evaluated. The freezing of the back-off counter when other station captures the channel was taken into account by this analytical model. In [36], a model was presented for performance evaluation of a protocol in multi hop ad hoc networks which considers most of the protocol's features.

Almasizadeh et al. [37] have used semi-Markov chains to quantify the security. The mean time to first security failure of the system, and the steady state security probabilities of the system were analyzed as security measures. However, the proposed method in [37] considers only one intrusion process while there are many intrusion processes in a system in real world. Ben-Othman et al. [38] have used SRNs to study the effect of different network factors on path connection availably in multi hop ad hoc networks.

3 Background Information

In this section, basic concepts and definitions of CTMCs and SRNs are presented. This section only intends to give some preliminaries on the concept of CTMCs and SRNs to be able to explain the proposed models and the methods of computing the mean time to attack detection and some other useful measures in the related context.

For more information about CTMCs and SRNs please see [17, 18, 39, 40] and [19, 20, 41], respectively.

3.1 Continuous Time Markov Chains

Stochastic models, in particular Markovian models, have been frequently used in the assessment of technical systems for performance, dependability, performability and survivability [39]. A stochastic process is a family of random variables, $X(t)$, defined on a sample space. The values assumed by $X(t)$ are called *states* and the set of all possible states is *state space* (S). The state space of a stochastic process can be discrete or continuous. In discrete state space, the corresponding stochastic process is called a *chain*. In addition to the state space, the time parameter of a stochastic process can be either discrete or continuous. If the time parameter is discrete (continuous), then the stochastic process is named discrete (continuous) time process [17]. A stochastic process can be also classified by the dependences of its state at a particular time on the states at previous times. According to this classification, a Markov process can be defined as a stochastic process in which each state of the process depends only on the immediately preceding state. If the state space, S, of a Markov process is discrete (finite or countably infinite), then the Markov process is known as Markov chain. More precisely, a Markov chain is a sequence of random variables X_1, X_2, X_3, ... with the Markov property, namely that, given the present state, the future and past states are independent. Formally,

$$Pr(X_{n+1} = x | X_1 = x_1, X_2 = x_2, ..., X_n = x_n) = Pr(X_{n+1} = x | X_n = x_n),$$

where the possible values of X_i are from the countable set of state space S [40].

If the time space of a Markov chain is continuous (discrete), the Markov chain is called continuous time (discrete time) Markov chain. The changes of states of a Markov chain are called transitions and the probabilities associated with these changes are named *transition probabilities*. In time homogeneous Markov chains in which the actual time instances are not important and only important matter is time instances' relative differences, the transition probabilities are independent of time but depend only upon the states [18, 40].

Let $(X(t), t \geq 0)$ represent a homogeneous finite state continuous time Markov chain (CTMC) with state space S. Let N be the number of states existing in $X(t)$. Then, the *generator matrix* of $X(t)$ can be written as an $N \times N$ matrix, $Q = [q_{ij}]$, in which each element q_{ij} represents the transition rate from state i to state j. Based on the definition of generator matrix in CTMCs, the diagonal elements of Q, q_{ii}, can be written as $-q_i$ which is equal to $\sum_{i \neq j} q_{ij}$. Let $P_i(t)$ denote the probability of being in state i at time t, so the state probability vector of $X(t)$ can be written as $P(t)$. Therefore, the transient behavior of $X(t)$ can be described by Eq. 1.

$$\frac{d}{dt}\big(P(t)\big) = P(t)Q, \qquad P(0) = p_0. \tag{1}$$

where p_0 is the initial probability vector of $X(t)$. In addition, the steady state probability vector of $X(t)$, represented by π, can be obtained by substituting $\frac{d}{dt}\big(P(t)\big) = 0$ in Eq. 1. Therefore, the steady state probability vector π can be computed using Eq. 2.

$$\pi Q = 0 \qquad \sum_{i \in S} \pi_i = 1. \tag{2}$$

where π_i is the steady state probability of being in state i of the CTMC $X(t)$.

As described above, the transient and steady state probabilities of being in state i of $X(t)$ can be computed by Eq. 1 and Eq. 2, respectively. Nevertheless, in some cases, it is necessary to compute the cumulative state probability of $X(t)$ [42]. Let $L_i(t)$ denote the expected total time spent by CTMC $X(t)$ in state i during the time interval $[0, t)$, then, the cumulative state probability vector of $X(t)$ can be computed using Eq. 3.

$$L(t) = \int_0^t P(\tau) d\tau \tag{3}$$

A more convenient way to calculate the cumulative state probabilities is the solution of differential equation Eq. 4.

$$\frac{d}{dt}\big(L(t)\big) = L(t)Q + P(0), \qquad L(0) = 0. \tag{4}$$

Closely related to the vector of cumulative state probabilities is the vector describing the time-average behavior of the CTMC as shown in Eq. 5.

$$M(t) = \frac{1}{t} L(t). \tag{5}$$

A CTMC is assumed to be an *absorbing* CTMC if it includes at least one *absorbing state*. A state $i \in S$ is said to be an absorbing state if and only if no other state of the CTMC can be reached from it [17]. In an absorbing CTMC it would be interesting to compute measures based on the time the CTMC spends in non-absorbing states before an absorbing state is ultimately reached. Let divide the state space S into two disjoint partitions A and N representing absorbing and non-absorbing states, respectively. Then, the time spent before absorption can be calculated by taking the limit $\lim_{t \to \infty} L_N(T)$ restricted to the states of the set N. In order to calculate $L_N(\infty)$, the generator matrix Q is restricted to those in N, so that matrix Q_N of size $|N| \times |N|$ is resulted. Restricting also the initial probability vector $P(0)$ to the non-absorbing states N results in $P_N(0)$, and allows the computation of $\lim_{t \to \infty}$ on both sides of differential equation Eq. 4, so that the following linear equation is resulted.

$$L_N(\infty) Q_N = -P_N(0). \tag{6}$$

With $L_N(\infty)$, the *mean time to absorption* ($MTTA$) can be computed as Eq. 7.

$$MTTA = \sum_{i \in N} L_i(\infty). \quad (7)$$

Assigning reward rate to each of the states of $X(t)$, a *Markov reward model* (MRM) can be constructed. Modeling a system using an appropriate CTMC and applying suitable reward rates to each of the states, one can compute some useful metrics such as the expected instantaneous and accumulated reward rates.

3.2 Stochastic Reward Nets

Petri Nets (PNs) are a graphical paradigm for the formal description of systems whose dynamics are characterized by concurrency, synchronization, mutual exclusion, and conflict, which are typical features of distributed environments [43, 44]. A Petri net can be defined as a 5-tuple:

$$PN = (P, T, F, W, M_0)$$

where
$P = \{p_1, p_2, ..., p_m\}$ is a finite set of *places*,
$T = \{t_1, t_2, ..., t_n\}$ is a finite set of *transitions*,
$F \subseteq (P \times T) \cup (T \times P)$ is a set of *arcs*,
$W : F \rightarrow \{1, 2, 3, ...\}$ is a *weight function*, and
$M_0 : P \rightarrow \{1, 2, 3, ...\}$ is the *initial marking*.

The Petri net graph model is a bipartite directed graph whose nodes are divided into two disjoint sets of places and transitions. The places and transitions are represented by circles and bars, respectively. The *marking* of a place is the number of tokens which the place contains. The marking of the Petri net is a vector that specifies the marking of each place in the net. A place is defined to be an input (output) place of a transition if there is an arc from the place (transition) to the transition (place). An integer ($d \geq 1$) called *arc multiplicity* is associated to each arc in the net. The default value for d is 1. A transition is said to be *enabled* if each of its input places contains at least as many tokens as that input arc's multiplicity. An enabled transition can $fire$. When a transition fires, it removes a number of tokens from each of its input places equal to the multiplicity of the corresponding arc and it deposits into each of its output places as many tokens as the multiplicity of the corresponding arc. Each firing generates a new marking of the net. Structural extensions to Petri nets include *inhibitor* arcs (denoted by an arc with a circle instead of an arrow head), which connect places to transitions. A transition can be enabled only if the number of tokens in its inhibitor place is less than the multiplicity of the inhibitor arc.

In the aforementioned definition, all transitions are the same and can fire as soon as they are enabled. The enabled transitions can fire and there is no priority among them. In other words, the firing of transitions is non-deterministic. In its basic form, PNs are adequate for verifying the system's properties, e.g., liveness, boundedness, invariants, and so forth. To allow a quantitative evaluation of the system's behavior, PNs have been extended in various ways to incorporate a time notion, such as timed Petri nets (TPNs). Basically, in PNs, time can be associated to the places (TPPNs) or transitions (TTPNs). These time-augmented Petri nets, TPPN as well as TTPN models, can be classified further depending upon whether the times mentioned are deterministic or stochastic. In the first case, the class of such Petri nets is called TPNs, and in the latter, they are called stochastic Petri nets (SPNs). Actually, SPNs are PNs in which we associate an exponentially distributed time delay with transitions [45]. In SPNs, all of the transitions are timed transitions. In order to overcome some quantitative problems existing in SPN analysis and model immediate actions in some systems, generalized stochastic Petri nets (GSPNs) have been introduced [44]. GSPNs have two different classes of transitions: *immediate* and *timed* transitions. Once enabled, immediate transitions fire in zero time. Timed transitions fire after a random, exponentially distributed enabling time as in the case of SPNs. In the graphical representation of GSPNs, immediate and timed transitions are drawn as bars and white rectangular boxes, respectively. A marking of a GSPN is said to be *vanishing* if at least one immediate transition is enabled in that marking and is said *tangible* otherwise.

A Stochastic Reward Net (SRN) is obtained by associating *reward rates* with markings of a GSPN [19]. SRN allows the automated generation of Markov Reward Models (MRM), making easy the combined evaluation of performance and dependability of degradable fault-tolerant systems. We associate a reward rate r_i with every tangible marking of the SRN, then the expected reward rate at steady state can be computed as $\sum_i r_i \pi_i$, where π_i denotes the steady state probability for the SRN to be in marking i. Several other extensions have been made in SRNs which include allowing multiplicity of arcs to be *marking dependent*, *enabling functions* or *guards* may be associated with transitions. SRN models can be automatically transformed into MRMs, and then, steady state and transient analysis of the obtained MRMs can produce the required measures of the original SRNs [19, 20, 41].

4 Problem Definition

In order to model the black-hole and gray-hole attacks in WANETs, the following assumptions are considered in this paper. These assumptions are commonly made in many research papers done in this research area [31, 46, 47, 48, 49, 50]. They can provide a general view of the network and type of the attacks, and help us to model the various aspects of the system and assess the useful measures exploiting the models.

- ***Assumption 1.*** There are a single specific source node and a specific destination node in the network. The source node acts as a sender and initiates the message broadcasting process, and the destination node acts as a receiver.
- ***Assumption 2.*** There are N independent intermediate nodes in the network which receive the *route request message* sent by the source node, and may reply this message with a fake *route reply message*.
- ***Assumption 3.*** The sending times of route request and route reply messages in both black-hole and gray-hole attacks follow exponential distribution.
- ***Assumption 4.*** There is an IDS in the network which can detect attack while m attacks are seen from a specific intermediate node. It is clear that the total number of attacks in the network may exceed the value of parameter m, but the IDS only detects the attack if all m attacks are done by a single node.
- ***Assumption 5.*** In the black-hole attack, if a route request message is attacked by an intermediate node, the other messages will be attacked by that node certainly. In other words, it is impossible to deliver a safe route request message to the destination node if the previous message has been attacked by an intermediate node.
- ***Assumption 6.*** In the black-hole attack, the attacker which attacks all route request messages is a single specific node.
- ***Assumption 7.*** In the gray-hole attack, it is possible to safely deliver the route request messages to the destination node even after the first attack. In other words, all attacks in the gray-hole attack are independent, and do not influence on each other.
- ***Assumption 8.*** In the gray-hole attack, the attacker may differ in each attack. However, the node which has attacked in previous phases is most prone to attack the other route request messages.

Considering the assumptions mentioned above, the proposed CTMC and SRN models are described in Section 5 and Section 6, respectively.

5 The Proposed CTMCs

The proposed CTMCs for modeling the black-hole and gray-hole attacks are presented in this section with details. The models realize the assumptions mentioned in Section 4.

5.1 The First Proposed CTMC

Figure 1 shows the proposed CTMC for the black-hole attack. The aim of this CTMC is to model sending a message from a single specific source to a given destination to find a route between the source and the destination while there are some intermediate nodes which may disturb this procedure by sending fake replies to the source pretending itself as the destination. *State* 1 and *state* 2 in the CTMC shown in Fig. 1 represent the initial states of the network in which a source node broadcasts a *route request message* to find a route. The message is assumed to be either safely received by the destination or attacked by one of the intermediate nodes existing in the network. Denoting p_1 and p_2 the probabilities of successful reception of the message by the destination and occurrence of an attack in the network, respectively, the CTMC will be in *state* 1 with probability p_1 and in *state* 2 with probability p_2 in the beginning. Let λ_1 and λ_2 denote the route request message sending rates whenever the message is delivered by the destination and intermediate nodes, respectively. Therefore, if the message is safely received by the destination, the CTMC transits from *state* 1 to *state* 3 with rate λ_1, otherwise, it transits to *state* 4 with rate λ_2.

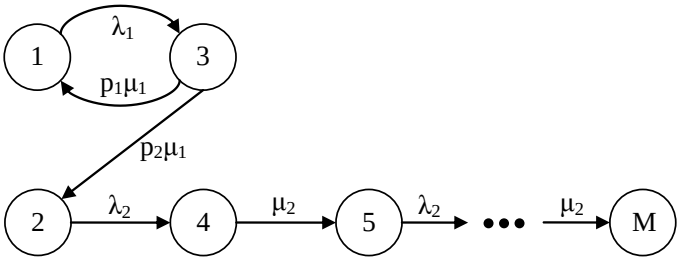

Figure 1 The proposed CTMC model for a black-hole attack

If the message is safely received by the destination, it replies this message with a new message called *route reply message*. Denoting μ_1 the route reply message sending rate, the CTMC shown in Fig. 1 transits from *state* 3 to *state* 1 and *state* 2 with rates $p_1\mu_1$ and $p_2\mu_1$, respectively. It emphasizes that the source node has broadcasted the next route request message after delivering the route reply message which may be safely delivered by the destination node (with probability p_1) or attacked by one of the intermediate nodes (with probability p_2). The probabilities p_1 and p_2 depend on the number of the intermediate nodes existing in the network. Increasing the number of the intermediate nodes, denoted by N, the attack probability, p_2, also increases. Therefore, appropriate values should be set for both probabilities p_1 and p_2 according to the value of N. One simple possibility is assigning the values $1 - \frac{N}{100}$ and $\frac{N}{100}$ to probabilities p_1 and p_2, respectively. These values satisfy the required condition in which increasing the value of N increases the probability of attack (p_2), and decreases the probability of safe delivering of message by the destination node (p_1).

In situation in which the message is attacked by an intermediate node, the source node would receive a fake reply from the attacker. Let μ_2 denote the fake

route reply message sending rate. Transition from *state* 4 to *state* 5 with rate μ_2 shows sending a fake route reply message to the source node by the attacker. After receiving the fake message by the source node, it starts a new session to check the existence of a route between itself and the destination. According to the *Assumption* 6 mentioned in Section 4, the same attacker will certainly attack the other route request messages sent by the source in next steps. Therefore, the proposed CTMC should transit from *state* 5 to the next state to represent the second attack in the network. It is worthwhile to mention that the rate of transition from *state* 5 to the next state is λ_2 which implies $p_1 = 0$ and $p_2 = 1$ after the first attack. Consequently, the CTMC transits to another state with rate μ_2 to start a new route request message sending phase. This procedure is continued till the predefined number of attacks (m) is occurred. After happening m attacks in the network by a specific intermediate node, the IDS detects the attack and the sequence finishes.

Variable M in the CTMC shown in Fig. 1 represents the number of the states of this CTMC ($|S|$). This variable is related to the number of the attacks which should be done by a single intermediate node to trigger IDS to detect the attack. As can be seen in Fig. 1, this variable is computed as $|S| = M = 2 + 1 + 2m = 1 + 2(m + 1)$ in which the last state, *state* M, is an absorbing state. In the CTMC proposed for the black-hole attack, there is only one absorbing state ($|A| = 1$), but the CTMC definitely reaches this state if it transits from *state* 2 to *state* 4 (occurring the first attack in the network). As an example, for an IDS which wishes to detect the attack after 3 times of attack occurrences ($m = 3$), we have $|S| = M = 9$ and $|A| = 1$. Increasing the number of attacks increases the number of states in the proposed CTMC. It should be noted that although the number of intermediate nodes does not influence the number of states directly, it highly influences the final result obtained from analyzing the proposed CTMC since it affects the value of both probabilities p_1 and p_2. The generator matrix Q of the CTMC shown in Fig. 1 can be written as Eq. 8.

$$
\mathrm{Q} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ \vdots \\ M \end{array}
\begin{array}{c}
\begin{array}{cccccc} 1 & 2 & 3 & 4 & \cdots & M \end{array} \\
\begin{pmatrix}
-\lambda_1 & 0 & \lambda_1 & 0 & \cdots & 0 \\
0 & -\lambda_2 & 0 & \lambda_2 & \cdots & 0 \\
p_1\mu_1 & p_2\mu_1 & -\mu_1 & 0 & \cdots & 0 \\
0 & 0 & 0 & -\mu_2 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 0
\end{pmatrix}
\end{array}
\tag{8}
$$

Using this matrix and applying Eq. 1, the transient state probability vector of the proposed CTMC can be computed when the initial probability vector is assumed as $P_0 = (p_1, p_2, 0, \cdots, 0)$. Moreover, the cumulative state probability vector can be computed using Eq. 3 and Eq. 4. The matrix Q_N discussed in Subsection 3.1 can also be achieved by removing both row and column M from the matrix Q shown in Eq. 8. Afterwards, the mean time to absorption ($MTTA$) of the proposed CTMC which represents the expected time required to detect an attack by IDS can be calculated by applying Eq. 7. $MTTA$ is a helpful measure in our study to estimate the time to detect an attack by the IDS which can be used in analyzing the IDS, and its sensitivity to other parameters of the system such as number of the intermediate nodes, number of the attacks which should be done by a single node to be able to detect an attack in the network, message sending and receiving rates and so forth. In addition to the measure $MTTA$, the probability of occurring k attacks in the network in time t, where $0 \leq k \leq m$, can be computed by analyzing the proposed CTMC.

5.2 The Second Proposed CTMC

Modeling a gray-hole attack using CTMCs is a little difficult compared to modeling a black-hole attack because of some differences existing between these two types of attacks. The differences are discussed in assumptions mentioned in Section 4, but in the following, two important differences are noted clearly.

- The intermediate node which attacked the first route request message may or may not attack the next route request messages in the gray-hole attack. Please remember that in the black-hole attack, the first attacker attacks all other route request messages, definitely. Therefore, there is a possibility of safely delivering next route request messages after the first attack by the destination which is ignored in the first CTMC shown in Fig. 1.
- In the gray-hole attack, the attackers belong to the pool of all intermediate nodes, and they are randomly selected from this pool. The second attacker may be different from the first attacker and the third attacker may be different from both the first and second attackers. Although the node which attacked before for some times is most tending to attack for the next times, the other nodes have the chance to attack the next route request messages, as well. It is different from the situation considered in the black-hole attack in which the attacker is fixed, and the node that attacked for the first time attacks the next messages in the next times surely.

In order to satisfy the specific requirements of a gray-hole attack, the CTMC shown in Fig. 2 is presented. *State* 1 and *state* 2 represent the initial states of the network such as the corresponding states of the first proposed CTMC. The route request message sent by the source node is either delivered by the destination node or attacked by one of the intermediate nodes in the network. If the message is delivered by the destination, the proposed CTMC transits from

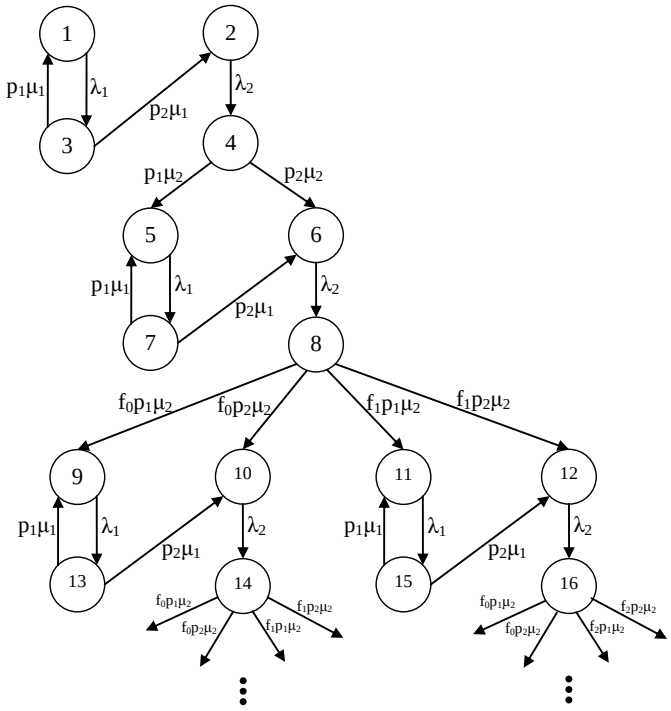

Figure 2 The proposed CTMC model for a gray-hole attack

state 1 to *state* 3; otherwise, it transits from *state* 2 to *state* 4. Probabilities p_1 and p_2, and all rates are the same as corresponding variables defined for the first proposed CTMC. As mentioned earlier, the probabilities p_1 and p_2 are functions of the number of the intermediate nodes in the network (N). The only condition for these probabilities is that increasing the number of the intermediate nodes should increase the attack probability (p_2), and decrease the safe delivering probability (p_1) proportionally.

If the message is safely delivered by the destination node, it is replied by a route reply message with rate μ_1. Since the next route request message will be safely delivered by the destination with probability p_1 and attacked by one of the intermediate nodes with probability p_2, the transition from *state* 3 to *state* 1 and *state* 2 is done with rates $p_1\mu_1$ and $p_2\mu_1$, respectively. If the first route request message is attacked by an intermediate node, the source node would receive a fake reply from the attacker. Therefore, the CTMC transits from *state* 4 to *state* 5 and *state* 6 with rates $p_1\mu_2$ and $p_2\mu_2$, respectively, to show that the next route request message can also be safely delivered by the destination node (*state* 5) or attacked by an intermediate node (*state* 6).

The aforementioned procedure is repeated among states 5, 7, and 6 which is basically similar to the procedure among states 1, 3, and 2. *State* 6 shows that the second attack is done by one of the intermediate nodes existing in the network. Transition from *state* 6 to *state* 8 represents sending the route request message from the source node which is delivered by one the intermediate nodes (the attacker). *State* 8 of the CTMC shown in Fig. 2 is very similar to the *state* 4 in which the attacker sends a fake route reply message to the source node and the procedure continues with applying probabilities p_1 and p_2 to the next route request message after the second attack. However, there is a subtle point here in that two different groups of intermediate nodes exist in *state* 8 unlike the intermediate nodes existing in *state* 4. In *state* 4, all of the intermediate nodes are the same in the viewpoint of attack at which none of them has attacked the messages, but in *state* 8 there are two groups of intermediate nodes; *group* 1) the pool of $N-1$ nodes which have not attacked the messages yet, and *group* 2) a node which has attacked for only one time. Therefore, the second attacker can be selected from either *group* 1 or *group* 2.

Let f_i denote the probability of attacking an intermediate node from the pool of the nodes which have attacked for i times. Therefore, in *state* 8, if a new intermediate node from the pool of $N-1$ nodes attacks the route request message as the second attack, CTMC transits from *state* 8 to *state* 9 or *state* 10; otherwise, it transits to *state* 11 or *state* 12. The selection is done probabilistically based on f_0, f_1, p_1 and p_2. Therefore, states 9 and 10 represent the situation in which two different intermediate nodes have attacked two route request messages separately, and states 11 and 12 represent the situation in which a given intermediate node has attacked two route request messages. It turns out that in all states 9 to 12, two attacks have been happened, but the difference is that in *state* 9 and *state* 10, the attacks have been done by two different intermediate nodes, and in *state* 11 and *state* 12, two attacks have been done by the same node.

The states 9, 13, and 10, and also the states 11, 15, and 12 are very similar to the states 5, 7, and 6 (or the states 1, 3, and 2). In *state* 14 and *state* 16, the third attack has been done and the fake route reply message is sent to the source node. In these cases, potential attackers should be considered before being able to properly transit to the other states with appropriate rates. In *state* 14, one possibility is attacking the message by one of the intermediate nodes existing in the pool of $N-2$ nodes which have not attacked yet. In this case, the CTMC transits from *state* 14 to the next states by two leftmost transitions shown in Fig. 2 with rates $f_0p_1\mu_2$ and $f_0p_2\mu_2$. Another possibility is attacking the message by one of the previous attackers. This case differs from the aforementioned cases in *state* 14. Since there is an intermediate node which attacked the previous messages for two times in *state* 14, the proposed CTMC transits from *state* 14 to the next states by two rightmost transitions with rates $f_1p_1\mu_2$ and $f_1p_2\mu_2$ to show that one of the intermediate nodes has attacked for two times. Similarly, we can discuss about *state* 16, in which the message is attacked by one of the intermediate nodes existing in the pool of $N-1$ nodes which have not attacked yet. In this situation, the CTMC transits from *state* 16 to the next states by two leftmost transitions with rates $f_0p_1\mu_2$ and $f_0p_2\mu_2$. The other possibility is

attacking the message by the previous attacker which has been attacked for two times. In this case, the proposed CTMC transits from *state* 16 to the next states by two rightmost transitions with rates $f_2 p_1 \mu_2$ and $f_2 p_2 \mu_2$.

This procedure is continued till all possible states of the CTMC are constructed. After generating all the state space, applying Eq. 1 and Eq. 2 to the resulted CTMC, the transient and steady state probability vectors of the CTMC can be computed, respectively. Moreover, the measure $MTTA$ can be estimated by applying Eq. 7. According to the combinations rules, the number of the states of the CTMC shown in Fig. 2 is computed by Eq. 9.

$$|S| = 4\binom{N+m-1}{N} + \binom{N+m-2}{N-1}. \tag{9}$$

Moreover, the number of the absorbing states ($|A|$) in this CTMC is computed using Eq. 10.

$$|A| = \binom{N+m-2}{N-1}. \tag{10}$$

As can be seen in Eq. 9 and Eq. 10, the number of all states ($|S|$) and absorbing states ($|A|$) in the second CTMC depend on both the number of intermediate nodes and the number of attacks which should be done by one node to trigger the IDS to detect the attack.

Since the number of attacks done by each of the intermediate nodes should be kept in each state, it is not easy to depict the overall CTMC for the gray-hole attack in general. In this case, each of the states with the potential attackers in that state should be considered to be able to draw the subsequent transitions and states. The CTMC shown in Fig. 2 represents a general case for only a few number of levels of the states and transitions. If we set the parameter m to 1, the *state* 5 will turn into an absorbing state, and the CTMC will contain only 5 states ($|S| = 5$ and $|A| = 1$). In this case, increasing the number of the intermediate nodes (N) does not influence the number of the states, because attacking only one intermediate node causes the net to be halted.

As another example, if we assume $N = 1$ and $m = 2$, the *state* 9 should be considered as an absorbing state. In this case, the number of the states is 9 which one of them is absorbing state ($|S| = 9$ and $|A| = 1$). When the values of the parameters N and m are set to large numbers, the number of the states in the proposed CTMC and its absorbing states become more than can be solved by hand. As an example, if we set the parameters N and m to 20 and 5, respectively, then the number of all and absorbing states in the state space will be $|S| = 51,359$ and $|A| = 8,855$ according to Eq. 9 and Eq. 10, respectively. It should be noted that these values for parameters N and m are conventional values in the real networks and IDSs. In order to overcome this shortcoming, we need an automatic way to generate the CTMC presented in Fig. 2. To fulfill this requirement, SRNs are used in the next section to automatically generate the proposed CTMCs, and compute the $MTTA$ of the CTMCs and other interesting measures.

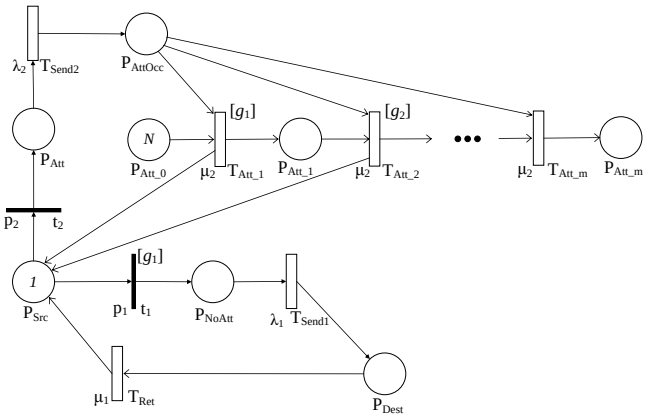

Figure 3 The proposed SRN model for a black-hole attack

6 The Proposed SRNs

The proposed SRNs for black-hole and gray-hole attacks similarly model sending a message from a source node to a destination node, and safe forwarding or dropping the messages. The proposed models take the same assumptions mentioned in Section 4 into consideration, and try to find the mean time to attack detection by analyzing the models. Moreover, other useful metrics are measured using transient analysis of the proposed SRNs. The most important advantage of the SRN models presented in this section is that the models can handle large numbers of intermediate nodes and different numbers of attacks. As discussed in Section 5, drawing and solving a CTMC modeling an IDS which deals with many intermediate nodes (large values of N) and detects a large number of attacks (large values of m) is almost impossible. However, the proposed SRNs can be easily used to automatically generate the corresponding CTMCs of the black-hole and gray-hole attacks, and manage different values of the parameters N and m.

6.1 The First Proposed SRN

The first SRN modeling the black-hole attack is shown in Fig. 3. Input parameters of the model are: (1) Number of the intermediate nodes (N), (2) sending rate of route request message delivered by the destination (λ_1), (3) sending rate of route request message delivered by an intermediate node (λ_2), (4) sending rate of real route reply message (μ_1), and (5) sending rate of fake route reply message (μ_2). It should be mentioned that the times assigned to all timed transitions follow exponential distribution as mentioned in *Assumption* 3.

The aim of the SRN shown in Fig. 3 is the same as the CTMC presented in Fig. 1 which is modeling the route request message sending process from a single specific source to a given destination to find a route between the source and destination. There are some intermediate nodes in the network which may disturb this procedure by sending fake replies to the source node. Places P_{Src} and P_{Dest} represent the source and destination nodes, respectively. There are two immediate

transitions, t_1 and t_2, connected to place P_{Src} which show the attack occurrence process. The probabilities p_1 and p_2 associated to immediate transitions t_1 and t_2, respectively, are the same as probabilities used in the CTMC shown in Fig. 1. As mentioned earlier, these probabilities depend on the parameter N at which increasing the value of N increases the probability p_2 and decreases p_1. Firing transition t_1 moves the net to the part related to successful delivering of route request message by the destination node, and firing transition t_2 moves the net to the attack occurrence and detection part. If immediate transition t_1 fires, a token is removed from place P_{Src} and a token is deposited into place P_{NoAtt} to show that the route request message will be safely delivered by the destination. Existing a token in place P_{NoAtt} enables timed transition T_{Send1} which represents the route request message sending process from the source node to the destination. Upon firing transition T_{Send1} with rate λ_1, a token is removed from place P_{NoAtt} and deposited into place P_{Dest} which enables timed transition T_{Ret}. Upon firing transition T_{Ret} with rate μ_1, a token is removed from place P_{Dest} and put in place P_{Src} representing a real route reply message has been sent to the source, and it is ready to start another route request session.

However, firing immediate transition t_2, a token is deposited into place P_{Att} which models occurrence of an attack in the network. Existence of a token in place P_{Att} enables timed transition T_{Send2} which models sending a route request message to the intermediate nodes. Upon firing timed transition T_{Send2} with rate λ_2, a token is removed from place P_{Att} and deposited into place P_{AttOcc}. Having a token in place P_{AttOcc} causes the timed transition T_{Att_1} to be enabled, since there are N tokens in place P_{Att_0}, and no tokens in places P_{Att_i}, $1 \leq i \leq m-1$, in the beginning. Place P_{Att_0} represents the intermediate nodes existing in the network which have not attacked yet. Firing transition T_{Att_1}, one token from place P_{AttOcc} together with another token from place P_{Att_0} is removed, and a token is deposited into both places P_{Att_1} and P_{Src}. Existing a token in place P_{Att_1} shows that an intermediate node has already attacked and sent a fake route reply message to the source node. As mentioned earlier, after attacking one intermediate node in the black-hole attack, the same node will certainly attack other route request messages sent by the source node in next steps. Therefore, in the first route request message after the first attack, transition t_1 cannot fire, and t_2 is the only enabled transition when there is a token in place P_{Src}. This is modeled using the guard function g_1 which prevents transition t_1 from firing when there is a token in at least one of the places P_{Att_i}, $1 \leq i \leq m-1$. This guard function is described in Table 1.

Having one token in place P_{AttOcc}, $N-1$ tokens in place P_{Att_0}, and one token in place P_{Att_1} in the second attack, both timed transitions T_{Att_1} and T_{Att_2} are enabled. To avoid transition T_{Att_1} from firing and provide the firing capability for transition T_{Att_2} in this situation, the guard function g_1 is also associated with transition T_{Att_1}. Hence, existing a token in place P_{Att_1} prevents transition T_{Att_1} to fire. Firing transition T_{Att_2}, one token is removed from all its input places and added to all its output places. Therefore, the source node can send another route request message after the second attack. In the third attack, we should prevent transition T_{Att_2} from firing to provide the firing capability for the subsequent timed transition named T_{Att_3} which is not depicted in Fig. 3. This is modeled by guard function g_2 described in Table 1 which prevents transition T_{Att_2} from firing when there is a token in at least one of places P_{Att_i}, $2 \leq i \leq m$. This procedure is continued till the number of attacks reaches the predefined threshold named m. In this case, transition T_{Att_m} fires and puts a token in place P_{Att_m}. Since the aim of the model is detecting m attacks in the network, the termination condition can be easily considered as existing a token in place P_{Att_m}. To do this, we do not return token to place P_{Src} which causes a halt in the net.

Table 1 Guard functions of the SRN model shown in Fig. 3

Guard Function	Value
g_i	1 if $\forall j_{i \leq j \leq m}[\#P_{Att\_j}] = 0$
$1 \leq i \leq m-1$	0 otherwise

Constructing the extended reachability graph of the SRN shown in Fig. 3 and specifying its rates and probabilities, the underlying Markov chain of this SRN model can be obtained which is the same as CTMC shown in Fig. 1. The interesting outputs in the proposed SRN are also the same as outputs introduced for the first proposed CTMC which are basically $MTTA$ and transient state probability vector of the underlying Markov chain. It is worthwhile to mention that the probabilities are defined on places in the SRN context which are finally translated to the corresponding probabilities and rewards in the underlying Markov chain by SRN supporting tools.

6.2 The Second Proposed SRN

The second SRN is shown in Fig. 4. In this SRN, a gray-hole attack is modeled at which an attacker may or may not attack the next route request messages after the first attack. To model this type of attacks, timed transitions T_{Att_i}, $1 \leq i \leq m$ of the first SRN are replaced with immediate transitions t_{Att_i}, $1 \leq i \leq m$, and two new components named P_{Ret} and T_{Ret2} are added to the net. Moreover, the guard functions and probabilities associated with some of the transitions are changed in the second SRN to be able to model the gray-hole attack.

The probability functions associated with transitions t_1 and t_2 of the second SRN are the same as functions defined for the first proposed SRN. Therefore, the first attack can be done as it has been described for the SRN shown in Fig. 3. In this case, if an attack occurred, transition t_2 fires and removes a token from place P_{Src}

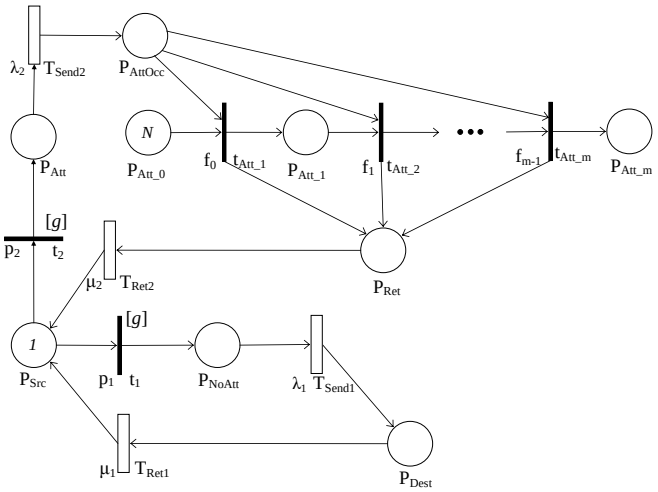

Figure 4 The proposed SRN model for a gray-hole attack

Table 2 Probability functions of transitions t_{Att_i}, $1 \leq i \leq m$ shown in the SRN model of Fig. 4

Probability	**Function**
f_i	$\frac{\alpha_i \cdot [\#P_{Att\_i}]}{\sum_{j=0}^{m-1} \alpha_j \cdot [\#P_{Att\_j}]}$
$0 \leq i \leq m-1$	$\alpha_j \in \mathbb{R}, 0 \leq j \leq m-1$

and deposits a token in place P_{Att}. Existing a token in place P_{Att} enables timed transition T_{Send2}. Upon firing transition T_{Send2}, a token is removed from place P_{Att} and put in place P_{AttOcc}. Existing a token in place P_{AttOcc} and N tokens in place P_{Att_0}, immediate transition t_{Att_1} fires. Firing this transition, a token is removed from both places P_{AttOcc} and P_{Att_0}, and added to both places P_{Ret} and P_{Att_1}. Existing a token in place P_{Ret}, timed transition T_{Ret2} is enabled. Once transition T_{Ret2} fires, a token is removed from place P_{Ret} and deposited into place P_{Src}. After the first attack, the source node sends a route request message which can be either safely received by the destination or attacked by one of the intermediate nodes according to the mechanism defined in the gray-hole attack. Therefore, in the case of attack, one of the intermediate nodes existing in the network can attack the route request message, and pretend itself as the destination node. This intermediate node can be assumed as one of the nodes which have not yet attacked ($N-1$ tokens inside place P_{Att_0}) or the node that has attacked for the first time (1 token inside place P_{Att_1}). Hence, having a token in place P_{AttOcc}, $N-1$ tokens in place P_{Att_0} and a token in place P_{Att_1} in the second attack, both immediate transitions t_{Att_1} and t_{Att_2} are enabled, and they can fire. The probability functions associated with enabled transitions t_{Att_i}, $1 \leq i \leq m$ are described in Table 2. For example, in situation that two transitions t_{Att_1} and t_{Att_2} are enabled, the probabilities f_0 and f_1 can be computed as Eq. 11 and Eq. 12, respectively.

$$f_0 = \frac{\alpha_0 \cdot [\#P_{Att\_0}]}{\alpha_0 \cdot [\#P_{Att\_0}] + \alpha_1 \cdot [\#P_{Att\_1}]} \tag{11}$$

$$f_1 = \frac{\alpha_1 \cdot [\#P_{Att\_1}]}{\alpha_0 \cdot [\#P_{Att\_0}] + \alpha_1 \cdot [\#P_{Att\_1}]} \tag{12}$$

where α_0 and α_1 are real numbers as mentioned in Table 2.

Eventually, after firing t_{Att_1} or t_{Att_2}, a token is deposited into place P_{Ret}, and then, the procedure continues. In the next route request messages, each of the intermediate nodes can also attack the message and pretend itself as the destination node. Thus, all tokens existing in places P_{Att_i}, $0 \leq i \leq m-1$ can be considered as potential attackers. In situation in which all transitions t_{Att_i}, $1 \leq i \leq m$ are enabled, one of them fires immediately based on the probabilities assigned to each of them. As can be seen in Table 2, the probability functions can easily handle the situations in which only one or more transitions are enabled. Assigning reasonable values for α_j, $0 \leq j \leq m-1$, we can model more realistic systems. For example, if we set $\alpha_0 = 1$, $\alpha_1 = 2$, and $\alpha_2 = 4$ for an SRN model with $m = 3$, it means that a node which has attacked for only one time will attack for the second time with the probability of two times greater than a node which have not attacked yet. Also, the probability of third attack by a given node is two and four times greater than the second and first attacks of a single node, respectively. In order to force the net to halt when the mth attack is done, the guard function g is associated with both immediate transitions t_1 and t_2. This guard function is shown in Table 3.

The SRN model presented in Fig. 4 generates a Markov chain such as one described in Subsection 5.2. This SRN can handle large values for both parameters N and m. Therefore, it can be used to model and evaluate most realistic situations in the network. After modeling the network and setting the appropriate values for input parameters of the proposed SRN for the gray-hole attack, interesting measures such as $MTTA$ and transient probability vector of the underlying Markov chain can be computed.

7 Numerical Results

Numerical examples are presented in this section to show the applicability of the proposed CTMCs and SRNs to compute the mean time to attack detection by an IDS in WANETs. In this paper, symbolic hierarchical automated reliability and performance evaluator (SHARPE) [51] and stochastic Petri net package (SPNP) [52] are used to solve the numerical examples of the proposed CTMCs and SRNs, respectively. Using these tools, $MTTA$ in both CTMC and SRN models, and transient and steady state probabilities of being in each of the states of the proposed CTMCs and the states of the underlying Markov chains of the proposed SRNs can be computed. To achieve this and compare

Table 3 Guard function of the SRN model shown in Fig. 4

Guard Function	Value
g	1 if $[\#P_{Att\_m}] = 0$ 0 otherwise

the results obtained from different situations, some scenarios are designed and implemented in SHARPE and SPNP. These scenarios are discussed in the following subsections with details.

7.1 Scenario 1: Black-hole Attack

In this scenario, black-hole attack is investigated, and two different measures are computed based on the experiments. The first measure is mean time to attack detection which is equivalent to $MTTA$ in both CTMC and SRN models. To do this, a network with N intermediate nodes which contains a single source and a single destination is assumed. The aim of the IDS in this scenario is detecting a black-hole attack when m consecutive attacks are done by a given intermediate node. The parameters λ_1 and λ_2 are set to 10 and 20, respectively, but generally, any value can be assigned to them. The only important issue is their proportion which should be set to an appropriate value. For example, we assume that the time required for delivering a route request message to the destination node is two times greater than the time required for delivering the message by one of the intermediate nodes in average. Moreover, it is supposed that λ_1=μ_1 and λ_2=μ_2, because both the request and reply messages transfer the same distance to be delivered by their destinations.

Figure 5 shows the mean time to attack detection for $m \in \{1, 2, \cdots, 5\}$. The horizontal axis of the plot shown in Fig. 5 represents the number of the intermediate nodes which varies from 10 to 50, and the vertical axis represents the mean time to attack detection. As can be seen in Fig. 5, the mean time to attack detection decreases when the number of intermediate nodes in the network increases (parameter N gets large numbers). It turns out that the value of parameter N influences on the probabilities p_1 and p_2 which affects the $MTTA$ in both CTMC and SRN models. It is worthwhile to mention that probabilities p_1 and p_2 are set to $1 - \frac{N}{100}$ and $\frac{N}{100}$, respectively. The bigger value for parameter N, the higher probability for attack occurrence will be resulted, and consequently, the lower mean time to attack detection is obtained. In addition to investigate the impact of parameter N on mean time to attack detection, the impact of parameter m can also be observed in Fig. 5. As it can be concluded from Fig. 5, the mean time to attack detection increases when the number of the attacks which is needed to be done by a single node to trigger the IDS to detect the attack (parameter m) increases. For example, the mean times to attack detection in a network with $N = 50$ intermediate nodes are about 0.3 and 0.7 when $m = 1$ and $m = 5$, respectively. The reason behind this result is that more

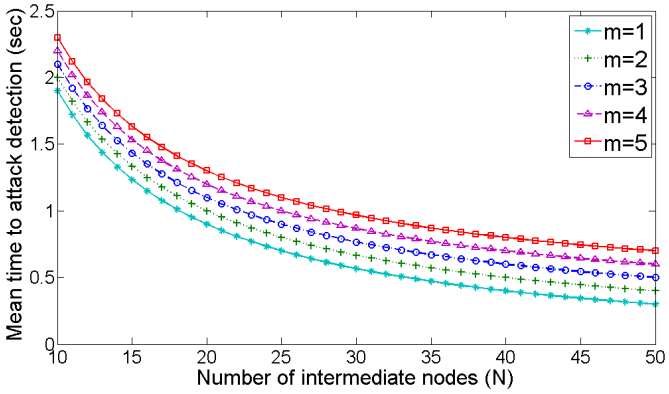

Figure 5 The mean time to attack detection in black-hole attack for different values of parameters N and m

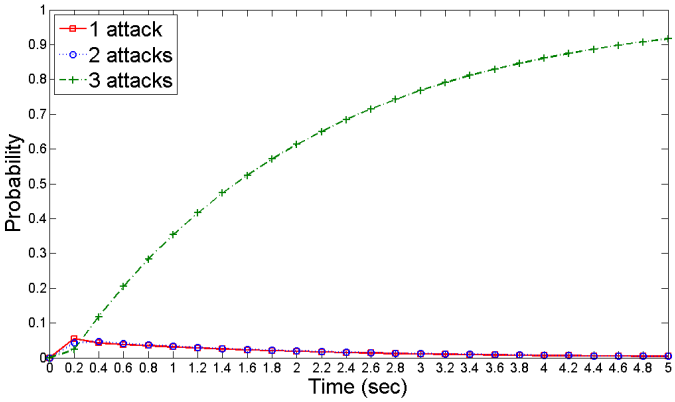

Figure 6 The probability of happening 1, 2, and 3 attacks in black-hole attack when $N = 10$ and $m = 3$

time is required for a single attacker to attack for m times when the parameter m is set to a bigger value.

Figure 6 shows the probability of happening 1, 2, and 3 attacks in a black-hole attack when the parameters N and m are set to 10 and 3, respectively. Since the mean time to attack detection for this setting is about 2.1, the horizontal axis showing the time variable is varied from 0 to 5 with incremental step 0.2. As can be seen in Fig. 6, the probabilities of occurring 1 and 2 attacks decrease when the time increases. Instead, the probability of occurring 3 attacks which finally results in absorbing the proposed CTMC and SRN models, increases when the time increases. It should be mentioned that this measure can be computed in both CTMC and SRN models using SHARPE and SPNP tools directly, but generally, computing this measure is very straightforward in SRN using SPNP. In SRN case, it suffices to compute the probability of existence a token in places P_{Att_i} when we wish to estimate the probability of happening i attacks in the network.

7.2 Scenario 2: Gray-hole Attack

In the scenario related to the gray-hole attack, different experiments are studied. In the first experiment, the

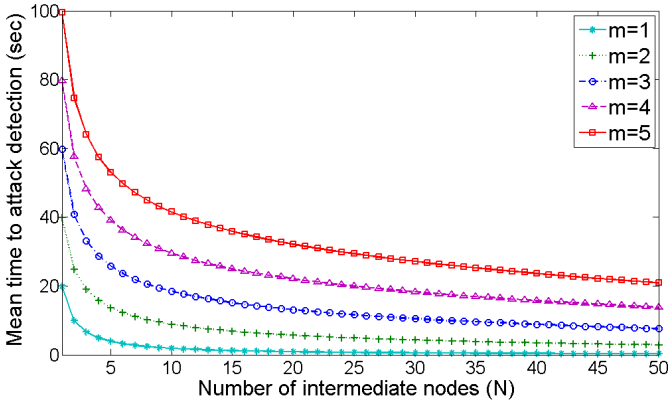

Figure 7 The mean time to attack detection in gray-hole attack for different values of parameters N and m where α_i=1, $\forall i, 0 \leq i \leq m-1$.

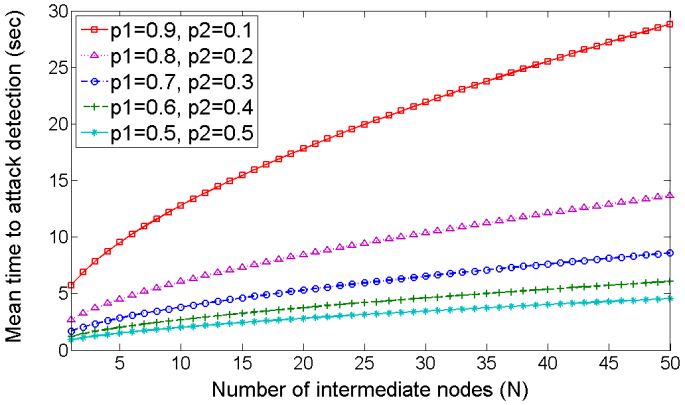

Figure 8 The mean time to attack detection in gray-hole attack for different values of parameter N where $m = 3$ and constant values are considered for probabilities p_1 and p_2

mean time to attack detection for different values of parameter N and $m \in \{1, 2, \cdots, 5\}$ is computed as same as the experiment for black-hole attack (Fig. 5). The result of this experiment is summarized in Fig. 7. In this experiment, all parameters α_i for $0 \leq i \leq m-1$ are set to 1. As a result, the probability of attacking an intermediate node from the pool of the nodes which have not attacked yet is equal to the probability of attacking a node which has been attacked for i times where $1 \leq i \leq m-1$. The values obtained for the mean time to attack detection in this experiment are very similar to the values shown in Fig. 5 for the black-hole attack in which the mean time to attack detection decreases when the number of intermediate nodes (N) increases. Moreover, this measure increases when the number of the attacks which is needed to be done by an intermediate node to trigger the IDS to detect the attack (parameter m) increases. Similar to the scenario related to the black-hole attack, in this experiment, the probabilities p_1 and p_2 are also set to $1 - \frac{N}{100}$ and $\frac{N}{100}$, respectively.

In the second and third experiments of the gray-hole attack, the parameter m is assumed to be a fixed number ($m = 3$) and the effects of probabilities p_1 and p_2, and parameters α_i to the mean time to attack detection are investigated. Figure 8 shows the mean time to attack detection for different number of intermediate nodes and different values of probabilities p_1 and p_2. As can be seen in Fig. 8, the values set for probabilities p_1 and p_2 are constant numbers, and they do not depend on the parameter N. Decreasing the value of probability p_1 (increasing the probability p_2), the mean time to attack detection decreases, because the probability of occurring an attack in the network by one of the intermediate nodes increases. Moreover, in this situation, increasing the number of the intermediate nodes in the network (N) increases the mean time to attack detection. This is against to the result shown in Fig. 7. The reason behind this result is that setting bigger values for parameter N when fixed probabilities are set for p_1 and p_2 implies the bigger values for probabilities f_i for smaller indexes. In other words, the probability of attacking a node with low number of attacks increases when the parameter N increases according to Table 2 which leads to the late absorption of the proposed CTMC and SRN models for gray-hole attack. It should be noted that in this case, the parameters α_1, α_2 and α_3 are 1, 2 and 4, respectively (please remember that $m = 3$ in Fig. 8).

Figure 9 shows the mean time to attack detection for different number of intermediate nodes and various values of parameter α_i, $0 \leq i \leq m-1$, where $m = 3$. As shown in Fig. 9, four different combinations for parameters α_i are considered where $\alpha_0 = 1$, $\alpha_1 = i$, $\alpha_2 = i^2$ and $i \in \{2, 3, 4, 5\}$. In this experiment, probabilities p_1 and p_2 are also set to $1 - \frac{N}{100}$ and $\frac{N}{100}$, respectively. Similar to the result shown in Fig. 7, the mean time to attack detection decreases when the number of intermediate nodes increases. It can be concluded from Fig. 9 that assigning bigger values for α_1 and α_2 leads to the lower mean time to attack detection. For example, if we set $\alpha_0 = 1$, $\alpha_1 = 5$ and $\alpha_2 = 25$, it means that a node that has attacked for only one time will attack for the second time with the probability of 5 times greater than a node which have not attacked yet. Moreover, the probability of third attack by a given node is 5 and 25 times greater than the second and first attacks of a single node, respectively. This setting provides higher chance for a node that has attacked for one time to attack for the second time compared to the setting in which $\alpha_1 = 4$ and $\alpha_2 = 16$.

Figure 10 shows the probability of happening 1, 2, and 3 attacks in a gray-hole attack when the parameters N and m are set to 10 and 3, respectively. In addition, in this experiment, probabilities p_1 and p_2 are $1 - \frac{N}{100}$ and $\frac{N}{100}$, respectively, and $\alpha_0 = 1$, $\alpha_1 = 2$, $\alpha_2 = 4$. Since the mean time to attack detection for this setting is about 13, the horizontal axis showing the time variable is varied from 0 to 30 with incremental step 1. As can be seen in Fig. 10, the probabilities of occurring 1 and 2 attacks start from *zero* and increase to reach a fixed value. These fixed values for occurring 1 and 2 attacks

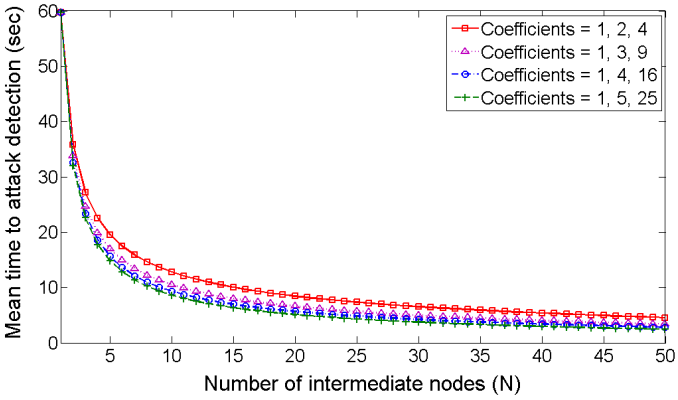

Figure 9 The mean time to attack detection in gray-hole attack for different values of parameter N where $m = 3$ and different values for $\alpha_i, 0 \leq i \leq m-1$ are considered

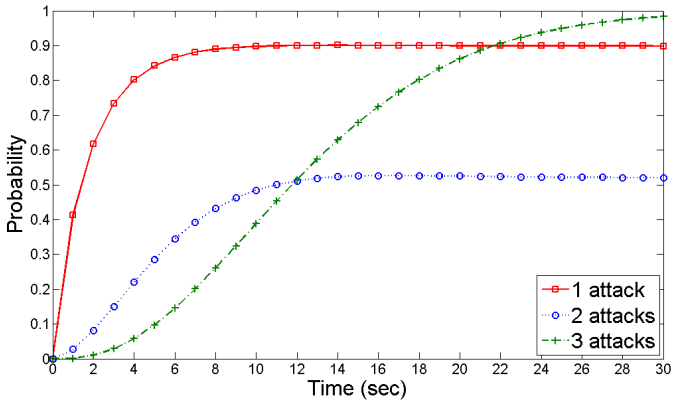

Figure 10 The probability of happening 1, 2, and 3 attacks in gray-hole attack when $N = 10$ and $m = 3$

are 0.90 and 0.52, respectively. However, the probability of occurring 3 attacks which finally leads to absorption in both CTMC and SRN models, increases to get 1 by increasing the time.

7.3 Scenario 3: Comparing Black-hole and Gray-hole Attacks

In this scenario, the experiments done for gray-hole and black-hole attacks are considered together. Figure 11 shows the mean time to attack detection for one black-hole and two gray-hole attacks. In all three experiments shown in Fig. 11, the parameter m is 3 and the number of intermediate nodes vary from 10 to 50. This figure shows the third case of the experiment shown in Fig. 5 named *Black hole*, the third case of the experiment shown in Fig. 7 named *Gray hole* 1, and the first case of the experiment shown in Fig. 9 ($\alpha_0 = 1$, $\alpha_1 = 5$, $\alpha_2 = 25$) named *Gray hole* 2 in a single plot. As can be seen in Fig. 11, the mean time to attack detection in black-hole attack is less than the related measure in both gray-hole attacks. This result is reasonable because in a black-hole attack, the attacker which has been attacked for the first

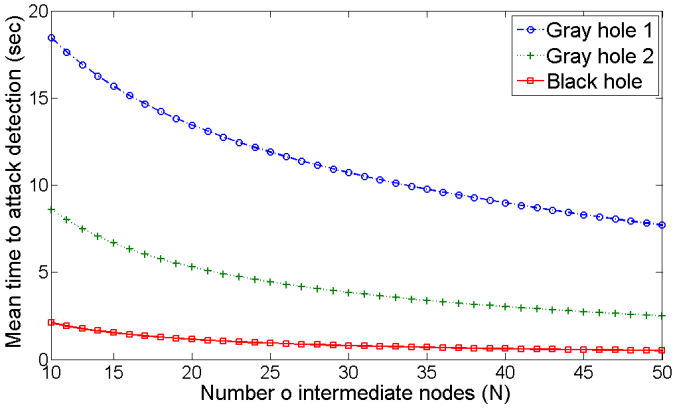

Figure 11 The mean time to attack detection in gray-hole and black-hole attacks where $m = 3$ and different values for parameter N are considered

time will attack the other route request messages in the future, but in the gray-hole attack there is a possibility of safely delivering the route request message to the destination node even after the first attack. Therefore, in both CTMC and SRN models, reaching the absorbing state(s) happens rapidly in black-hole attack compared to the both gray-hole attacks.

In addition to comparing black-hole and gray-hole attacks, two different settings in the case of gray-hole attack can be compared using the plot shown in Fig. 11. As can be concluded from Fig. 11 (and considering Fig. 9), when it is assigned a higher attack probability to the nodes which have attacked already compared to the nodes which have not attacked yet, more precisely $\alpha_{i+1} > \alpha_i$, $\forall i, 0 \leq i \leq m-2$, the mean time to attack detection becomes a small value, and converges to the related measure in the black-hole attack.

8 Conclusions and Future Work

Wireless network is always a target of different passive and active attacks which may harm the security of the network. Black-hole and gray-hole are two important active attacks which try to scratch the availability attribute of the security in this kind of networks. To detect such attacks, IDS can be used as a very effective mechanism. In order to evaluate the performance of the IDSs, we model IDSs within WANETs using CTMCs and SRNs. The mean time to attack detection and probability of happening i attacks in the network at time t are two important measures which can be assessed using our proposed models. Numerical examples are used to show different settings of IDSs and their effectiveness where the number of intermediate nodes and the number of attacks in the network are taken into account.

There are some open problems in this area which are interesting to solve. The first important issue is improving the models to handle different number of attacks in a single SRN (and consequently a CTMC). In current SRN models, the number of attacks which

should be done by a single node to trigger the IDS to detect the attack is modeled by a sequence of places and transitions in both black-hole and gray-hole attacks. The difficulty with this method is the scalability issue of the proposed models. If the number of attacks is changed, the whole SRN model should be changed to handle the new value. In the proposed SRN models, the number of intermediate nodes are shown with tokens inside a place which makes the model more scalable. One possible solution for improving the scalability of the models in the viewpoint of the number of attacks is modeling the attacks with tokens inside the net as same as the intermediate nodes. Using this mechanism, the models can handle different numbers of intermediate nodes and attacks by a single structure.

The second important subject which can be considered as a topic of another related research is modeling several IDSs together, and then, relating the models to each other to reflect the cooperation among the IDSs. Existing several IDSs in a network which cooperate with each other to find the attacker can also be modeled using SRNs. In this case, the mean time to attack detection will decrease because IDSs can inform each other from the status of each of the intermediate nodes, and finally, detect the attack faster. Moreover, using high level extensions of Petri nets and activity networks such as colored extensions, it is possible to recognize the attacker from the pool of intermediate nodes.

References

[1] C. Zhang, Y. Song, Y. Fang, and Y. Zhang. On the price of security in large-scale wireless ad hoc networks. *IEEE/ACM Transactions on Networking*, 19(2):319–332, 2011.

[2] M. Nogueira, H. Silva, A. Santos, and G. Pujolle. A security management architecture for supporting routing services on WANETs. *IEEE Transactions on Network and Service Management*, 9(2):156–168, 2012.

[3] H. Wenbo, H. Ying, R. Sathyam, K. Nahrstedt, and W.C. Lee. SMOCK: A scalable method of cryptographic key management for mission-critical wireless ad-hoc networks. *IEEE Transactions on Information Forensics and Security*, 4(1):140–150, 2009.

[4] I. Aad, J.-P. Hubaux, and E.W. Knightly. Impact of denial of service attacks on ad hoc networks. *IEEE/ACM Transactions on Networking*, 16(4):791–802, 2008.

[5] S. Djahel, F. Nait-abdesselam, and Z. Zonghua. Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges. *IEEE Communications Surveys and Tutorials*, 13(4):658–672, 2011.

[6] Q. Liu, J. Yin, V. Leung, and Z. Cai. FADE: forwarding assessment based detection of collaborative grey hole attacks in WMNs. *IEEE Transactions on Wireless Communications*, PP(99):1–14, 2013.

[7] T. Anantvalee and J. Wu. A survey on intrusion detection in mobile ad hoc networks. In Y. Xiao, X.S. Shen, and D.-Z. Du, editors, *Wireless Network Security*, Signals and Communication Technology, pages 159–180. Springer, 2007.

[8] J.-H. Cho, I.-R. Chen, and P.-G. Feng. Effect of intrusion detection on failure time of mission-oriented mobile group systems in mobile ad hoc networks. In *The 14th IEEE Pacific Rim International Symposium on Dependable Computing*, pages 289–296, Taipei, Taiwan, 15–17 December 2008.

[9] K. Gulshan. Evaluation metrics for intrusion detection systems - a study. *International Journal of Computer Science and Mobile Applications*, 2(11):11–17, 2014.

[10] M. Alikhany and M. Abadi. A dynamic clustering-based approach for anomaly detection in AODV-based MANETs. In *International Symposium on Computer Networks and Distributed Systems (CNDS)*, pages 67–72, Tehran, Iran, 23–24 February 2011.

[11] A.F. Farhan, D. Zulkhairi, and M.T. Hatim. Mobile agent intrusion detection system for mobile ad hoc networks: A non-overlapping zone approach. In *The 4th IEEE/IFIP International Conference on Internet*, pages 1–5, Tashkent, Uzbekistan, 23–25 September 2008.

[12] S. Buchegger and J.-Y.L. Boudec. Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*.

[13] B. Shengrong, F.R. Yu, X.P. Liu, P. Mason, and H. Tang. Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. *IEEE Transactions on Vehicular Technology*, 60(3):1025–1036, 2011.

[14] J.P. Magalhaes and L.M. Silva. Anomaly detection techniques for web-based applications: An experimental study. In *The 11th IEEE International Symposium on Network Computing and Applications (NCA)*, pages 181–190, August 2012.

[15] S.K. Sharma J.N.D. Gupta. *Handbook of Research on Information Security and Assurance*. IGI Global Press, first edition, 2009.

[16] M. Cramer, J. Cannady, and J. Harrell. New methods of intrusion detection using control-loop measurement. In *Proceedings of the Technology in Information Security Conference*, volume 95, pages 1–10, 1995.

[17] G. Bolch, S. Greiner, H.d. Meer, and K.S. Trivedi. *Queueing Networks and Markov Chains: Modeling and Performance Evaluation with Computer Science Applications*. John Wiley and Sons, second edition, 2006.

[18] V. Cardellini, E. Casalicchio, K.R.L. Jaquie, C. Branco, J.C. Estrella, and F.J. Monaco. *Performance and Dependability in Service Computing: Concepts, Techniques and Research Directions*. IGI Global, first edition, 2012.

[19] J.K. Muppala and K.S. Trivedi. Composite performance and availability analysis using a hierarchy of stochastic reward nets. In G. Balbo and G. Serazzi, editors, *Computer Performance Evaluation, Modelling Techniques and Tools*, pages 335–349. Elsevier Science Publishers B.V. (North-Holland), 1992.

[20] G. Ciardo and K.S. Trivedi. A decomposition approach for stochastic reward net models. *Performance Evaluation*, 18(1):37–59, 1993.

[21] M. Medadian, M.H. Yektaie, and A.M. Rahmani. Combat with black hole attack in AODV routing protocol in MANET. In *First Asian Himalayas International Conference on Internet*, pages 1–5, Kathmandu, Nepal, 3–5 November 2009.

[22] X.Y. Zhang, Y. Sekiya, and Y. Wakahara. Proposal of a method to detect black hole attack in MANET. In *International Symposium on Autonomous Decentralized Systems*, pages 1–6, Athens, Greece, 23–25 March 2009.

[23] G. Xiaopeng and C. Wei. A novel gray hole attack detection scheme for mobile ad-hoc networks. In *IFIP International Conference on Network and Parallel Computing Workshops*, pages 209–214, Liaoning, China, 18–21 September 2007.

[24] J. Sen, M.G. Chandra, S.G. Harihara, H. Reddy, and P. Balamuralidhar. A mechanism for detection of gray hole attack in mobile ad hoc networks. In *The 6th International Conference on Information, Communications Signal Processing*, pages 1–5, Singapore, 10–13 December 2007.

[25] A. Mitrokotsa, N. Komninos, and C. Douligeris. Intrusion detection with neural networks and watermarking techniques for MANET. In *IEEE International Conference on Pervasive Services*, pages 118–127, Istanbul, Turkey, 15–20 July 2007.

[26] W. Scheirer and M.C. Chuah. Syntax vs. semantics: Competing approaches to dynamic network intrusion detection. *International Journal of Security and Networks*, 3(1):24–35, 2008.

[27] K. Chang and K.G. Shin. Application-layer intrusion detection in MANETs. In *The 43rd Hawaii International Conference on System Sciences (HICSS)*, pages 1–10, Honolulu, Hawaii, 5–8 January 2010.

[28] B. Shengrong, F.R. Yu, X.P. Liu, and H. Tang. Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks. *IEEE Transactions on Wireless Communications*, 10(9):3064–3073, 2011.

[29] Y. Ping, J. Xinghao, W. Yue, and L. Ning. Distributed intrusion detection for mobile ad hoc networks. *Journal of Systems Engineering and Electronics*, 19(4):851–859, 2008.

[30] J. Cho, I. Chen, and V. Tech. Performance analysis of distributed intrusion detection protocols for mobile group communication systems. In *The IEEE International Symposium on Parallel and Distributed Processing*, pages 1–8, Rome, Italy, 23–29 May 2009.

[31] H. Huang and Q. Zhou. Petri-net-based modeling and resolving of black hole attack in WMN. In *The IEEE 36th Annual Computer Software and Applications Conference Workshops*, pages 409–414, Izmir, Turkey, 16–20 July 2012.

[32] M. Dasgupta, D. Santra, and S. Choudhury. Network modelling of a black-hole prevention mechanism in mobile ad-hoc network. In *The 4th International Conference on Computational Intelligence and Communication Networks*, pages 734–738, Mathura, India, 3–5 November 2012.

[33] M.A. Azgomi and A. Khalili. Performance evaluation of sensor medium access control protocol using coloured petri nets. In *The 1st International Workshop on Formal Methods for Wireless Systems*, pages 66–76, Toronto, Canada, 23 August 2008.

[34] A. Sedaghatbaf and M.A. Azgomi. Attack modeling and security evaluation based on stochastic activity networks. *Security and Communication Networks*, 7(4):714–737, 2014.

[35] R. Jayaparvathy, S. Anand, S. Dharmaraja, and S. Srikanth. Performance analysis of IEEE 802.11 DCF with stochastic reward nets. *International Journal of Communication Systems*, 20(3):273–396, 2007.

[36] O. Younes and N. Thomas. An SRN model of the IEEE 802.11 DCF MAC protocol in multi-hop ad

hoc networks with hidden nodes. *The Computer Journal*, 54(6):875–893, 2011.

[37] J. Almasizadeh and M. A. Azgomi. Intrusion process modeling for security quantification. In *International Conference on Availability, Reliability and Security*, pages 114–121, Fukuoka, Japan, 16–19 March 2009.

[38] J. Ben-Othman, S. Diagne, B. Yahya, and L. Mokdad. Performance evaluation of a medium access control protocol for wireless sensor networks using petri nets. *Electronic Notes in Theoretical Computer Science*, 242:335–354, 2010.

[39] M.G. McQuinn, P. Kemper, and W.H. Sanders. Dependability analysis with markov chains: How symmetries improve symbolic computations. In *The 4th International Conference on the Quantitative Evaluation of Systems*, pages 151–160, Edinburgh, UK, 17–19 September 2007.

[40] B.R. Haverkort. Markovian models for performance and dependability evaluation. In E.Brinksma, H. Hermanns, and J.-P. Katoen, editors, *Lectures on Formal Methods and Performance Analysis*, volume 2090 of *Lecture Notes in Computer Science*, pages 38–83. Springer, 2001.

[41] H. Sun and K.S. Trivedi. A stochastic reward net model for performance analysis of prioritized DQDB MAN. *Computer Communications*, 22(9):858–870, 1999.

[42] K.S. Trivedi, G. Ciardo, M. Malhotra, and R.A. Sahner. Dependability and performability analysis. In L. Donatiello and R. Nelson, editors, *Performance Evaluation of Computer and Communication Systems*, volume 729 of *Lecture Notes in Computer Science*, pages 587–612. Springer, 1993.

[43] J. L. Peterson. *Petri Net Theory and the Modeling of Systems*. Prentice Hall, first edition, 1981.

[44] M.A. Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis. *Modeling with Generalized Stochastic Petri Nets*. John Wiley and Sons, first edition, 1995.

[45] F. Bause and P. S. Kritzinger. *Stochastic Petri Nets: An Introduction to the Theory*. Vieweg+Teubner Verlag, second edition, 2002.

[46] J. Liu, X. Jiang, H. Nishiyama, and N. Kato. On the delivery probability of two-hop relay MANETs with erasure coding. *IEEE Transactions on Communications*, 61(4):1314–1326, 2013.

[47] A.A. Hanbali, P. Nain, and E. Altman. Performance of ad hoc networks with two-hop relay routing and limited packet lifetime (extended version). *Performance Evaluation*, 65(6–7):463–483, 2008.

[48] X. Chen, K. Makki, K. Yen, and N. Pissinou. Attack distribution modeling and its applications in sensor network security. *EURASIP Journal on Wireless Communications and Networking*, 2008:1–11, 2008.

[49] I. Gruber and H. Li. Link expiration times in mobile ad-hoc networks. In *The 27th Annual IEEE Local Computer Networks Conference*, pages 743–750, Tampa, Florida, US, 6–8 November 2002.

[50] F. Bai, N. Sadagopan, and A. Helmy. The important framework for analyzing the impact of mobility on performance of routing protocols for ad hoc networks. *Ad Hoc Networks*, 1(4):383–403, 2003.

[51] R. Sahner, K.S. Trivedi, and A. Puliafito. *Performance and Reliability Analysis of Computer Systems An Example-Based Approach Using the SHARPE Software Package*. Kluwer Academic Publishers, first edition, 1996.

[52] G. Ciardo, J.K. Muppala, and K.S. Trivedi. SPNP: Stochastic petri net package. In *The 3rd International Workshop on Petri Nets and Performance Models*, pages 142–151, Kyoto, Japan, December 1989.