# Intelligent Internal Stealthy Attack and its Countermeasure for Multicast Routing Protocol in MANET

Menaka Pushpa Arthur and Kathiravan Kannan

**Multicast communication of mobile ad hoc networks is vulnerable to internal attacks due to its routing structure and high scalability of its participants. Though existing intrusion detection systems (IDSs) act smartly to defend against attack strategies, adversaries also accordingly update their attacking plans intelligently so as to intervene in successful defending schemes. In our work, we present a novel indirect internal stealthy attack on a tree-based multicast routing protocol. Such an indirect stealthy attack intelligently makes neighbor nodes drop their routing-layer unicast control packets instead of processing or forwarding them. The adversary targets the collision avoidance mechanism of the Medium Access Control (MAC) protocol to indirectly affect the routing layer process. Simulation results show the success of this attacking strategy over the existing "stealthy attack in wireless ad hoc networks: detection and countermeasure (SADEC)"detection system. We design a cross-layer automata-based stealthy attack on multicast routing protocols (SAMRP) attacker detection system to identify and isolate the proposed attacker. NS-2 simulation and analytical results show the efficient performance, against an indirect internal stealthy attack, of SAMRP over the existing SADEC and BLM attacker detection systems.**

**Keywords: MAODV, BLM, SADEC, multicast communication, SAMRP, stealthy attack.**

Manuscript received Aug. 24, 2014; revised Aug. 10, 2015; accepted Aug. 21, 2015.

Menaka Pushpa Arthur (corresponding author, menaka_engg@yahoo.com) and Kathiravan Kannan (kathirraji@gmail.com) are with the Department of Computer Science and Engineering, Easwari Engineering College, Anna University, Chennai, India.

## I. Introduction

Security issues of multicast routing protocols in mobile ad hoc networks (MANETs) need extensive research, focusing specifically on improving their robustness against all types of internal attacks. Many techniques have been proposed to secure unicast communication for use in MANETs. However, multicast routing protocols follow their own unique approach in routing operations to construct multicast routing structures, and as a result, existing unicast security techniques cannot be applied to protect multicast communication from various vulnerabilities. In addition, previous research works [1]–[9] have justified the requirement of dedicated countermeasures by multicast routing protocols against both internal and external attacks in MANETs. Existing attacker prevention techniques of multicast routing protocols suffer from high communication overhead and enormous delay, as explained by Mo'men and others [9]. Attacker prevention techniques such as these should be enhanced so as to be able to classify misbehaving nodes and legitimate nodes under a network's challenging conditions, such as high traffic, density, and mobility. Intelligent observation of a node's behavior in normal and attacker network scenarios is needed to detect internal adversaries in a multicast communication environment. Different types of internal attacks on tree- and mesh-based multicast routing protocols are discussed in [1]–[4], [8], and [10]–[11]. Khalil and Bagchi [12] introduced a suite of *stealthy* attacks for unicast routing protocols used in MANETs and successfully mitigated them using the SADEC protocol. A stealthy attack in wireless ad hoc networks: detection and countermeasure

  
http://dx.doi.org/10.4218/etrij.15.0114.1011

(SADEC) mitigation technique was designed specifically to address stealthy attacks such as packet misrouting and those that are of the power control type [12].

In our work, we present a novel indirect internal stealthy attack similar in intention to that of the colluding-collision attack of Issa and others [13], the only difference being that our attacking strategy is completely different. By exploiting the RTS/CTS handshake protocol, an indirect internal stealthy attack can be launched by multicast group members. We analyze the impact of this attack on a familiar tree-based multicast routing protocol, multicast ad-hoc on-demand distance vector (MAODV) [13]. Our work is the first research work of its kind to introduce a stealthy attack on multicast routing protocols (SAMRPs) intended for use in MANETs. We discover that the location of the attacker in the network makes a major difference in its attacking gain on multicast services. Our simulation results show that the SADEC protocol cannot detect this type of stealthy attack from multicast communication. So, we propose an efficient detection and isolation technique, SAMRP, designed specifically to refute an attack of this nature. This detection technique is built upon on a local monitoring system similar to that found in SADEC, with the proposed system being able to combine with multicast communication to detect an attacker by extending observations in the medium access control (MAC) layer. An automata-based attacker detection technique is used to detect abnormal patterns from an observed traffic window. Simulation results show that the proposed SAMRP technique successfully detects a stealthy attacker from a multicast group, with more true positives and false positives than SADEC. This work is the extension of our previous paper [14].

The remainder of this paper is organized as follows. Section II discusses the related works. Section III explains the proposed attacking strategy on MAODV. Our cross-layer-based stealthy attacker detection technique, SAMRP, is presented in Section IV. A theoretical analysis of an attacker's impact and effectiveness on the proposed system is discussed in Section V. Extensive simulations have been carried out to analyze the impact of an internal stealthy attack, and performance measures of the proposed SAMRP are presented in Section VI. Section VII concludes this paper.

## II. Related Works

The importance of multicast communication in group-based activities of MANETs is explained in [15]. Multicast communication of MANETs is a special type of broadcast communication in that it does not utilize the collision avoidance mechanism of the IEEE 802.11 MAC [16]–[19] due to the high scalability of its participants. This issue has been analyzed by Obraczka and Tsudik [1]; Mohapatra and others [15]; and L.K. Law and others [20]. Very limited research works have been contributed for discussing the security issues of multicast routing protocols in MANETs. The possible attacks on MAODV [13] have been identified and explained in [2]–[8]. However, these studies concentrate only on internal attacks common to both unicast and multicast routing protocols, such as black hole, worm hole, and rushing attacks. Very few works proposed by [9] and [6] have identified multicast-specific security attacks on multicast routing protocols of MANETs. Most of the existing research work, except for [3], [5], [8], [10], [11], fails to explore the vulnerabilities of multicast communication in MANETs. Window-based anomaly detection in network traffic is presented by Wattenbergand others [21] and O'Reilly and others [22]. Misra and others [23] and Yu and others [24] designed an automaton to detect anomaly patterns from network traffic.

## III. Indirect Internal Stealthy Attack on MAODV

### 1. Network Model

Let us assume that a network consists of a number of wireless mobile nodes, $N$. Each node has a fixed transmission range, $r$, and transmission powers in both transmit and receive process. Wireless links are symmetric in between any given pair of nodes. A pair of nodes can communicate with each other if they are both located within one of their transmission ranges ($r$), and they are both assumed to use a random-walk mobility model. Key-based secure communication between multicast group members is beyond the scope of this paper. The number of multicast groups in the network is represented by |MG|. Each multicast group has a set of nodes, $M_i$, that is the union of two sets, $R_i$ and $S_i$, in which $S_i$ is a singleton; $R_i$ is a set of receivers and $S_i$ is a unit set with a source from multicast group $i$. We have $M_i = R_i \cup S_i$, $R_i$, and $S_i$ as the subsets of set $M_i$ (that is, $R_i \subseteq M_i$ and $S_i \subseteq M_i$). Also, $T_i$ represents a set of tree nodes in multicast group $i$, and it is the union of two sets, $M_i$ and $NM_i$ (that is, $T_i = M_i \cup NM_i$). Here, $\mathrm{NM}_i$ is the set of non-group members existing in the multicast tree of multicast group $i$. Note that $M_i$ and $\mathrm{NM}_i$ form a symmetric difference set; that is, $NM_i \cap M_i = \emptyset$. Note also that $M_i$ is a proper subset of $T_i$ ($T_i \subset M_i$ in some topologies of the network); whereas, $NM_i$ is always a subset of $T_i$, and $\mathrm{NM}_i \in N$.

### 2. Attacker Model

In this work, we concentrate only on indirect stealthy attacks against multicast routing protocols of MANETs. Transport and physical layer attacks on multicast routing protocols are beyond the scope of this paper. In our attacking model, we

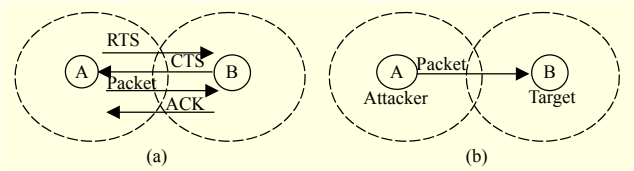



Fig. 1. Example of attack model: (a) RTS/CTS mechanism for unicast packet forwarding and (b) indirect internal stealthy attacker.

introduce a novel indirect internal stealthy attack that makes legitimate nodes drop received routing-layer unicast control packets by wrongly exploiting the RTS/CTS mechanism at the MAC source. Normal and adversarial unicast packet transmission mechanisms are shown in Figs. 1(a) and 1(b), respectively. This attacking strategy falls under the category of "cross-layer (routing and MAC layer) security attacks" in multicast routing protocols. Attackers are randomly selected from multicast tree members, except the multicast source.

## 3. Proposed Indirect Internal Stealthy Attack

An indirect internal stealthy attack creates a situation where the intended legitimate MAC-receiver drops the received unicast route discovery control packets instead of forwarding or processing them. Here, the attacker plays the role of MAC-sender and the intended legitimate MAC-receiver is a target node. The attacker widens their attacking strategy to include the MAC and routing layers of MAC-sender and MAC-receiver. The main objectives of an indirect internal stealthy attack are as follows:

- An attacker does not directly drop packets, but can succeed with their plan of attack.
- Makes a legitimate MAC-receiver drop unicast route discovery control packets received from its attacker's neighbors.
- An attacker can survive without being caught by a conventional intrusion detection system (IDS), whereas a legitimate node is to be punished for its packet-dropping malicious activity.

The indirect internal stealthy attacking strategy on MAODV is very intelligent, the attack being triggered against the collision avoidance mechanism of the IEEE 802.11 MAC protocol [19]. An attacker does not follow the RTS/CTS handshake mechanism instructed by this protocol before it transmits unicast packets. The "sendRTS()" function of the MAC protocol is called to create and transmit an RTS packet in the case of a unicast packet. The RTS/CTS handshake protocol is used only when a transmitting packet is of unicast type and its size greater than an "RTS_threshold" value. This condition imposed by the IEEE 802.11 MAC protocol is exploited by the indirect stealthy attacker. The attacker executes "sendRTS( )," within which it frees the created RTS packet by falsely claiming the packet size to be less than the "RTS_threshold" value. Then, unicast packets are sent to the MAC-receiver without a collision avoidance mechanism.

The last stage of the attacking plan is carried out by a legitimate MAC-receiver. Normally, a MAC receiver drops received unicast packets, instead of processing them, on the condition that its previous packet was not a CTS packet and that it was not sent to a MAC-source. The IEEE 802.11 MAC protocol insists that the MAC receiver drops the packets if its previous state is not that of "MAC_CTS." Unfortunately, the MAC receiver cannot recognize the actual reason behind this activity and the IEEE 802.11 MAC protocol cannot differentiate between the attacker's strategy and the unintended MAC routing flaws. The MAC sender (that is, the attacker) attempts to retransmit the unicast packet a given number of times if it does not receive an acknowledgement packet from the MAC receiver in an attempt to maintain a legitimate image. When the maximum retry count is exceeded, the packet is dropped by the source node, with the reason stated by the source for this drop being "failure to transmit the packet within maximum attempt." A small malfunction triggered by an attacker induces major performance degradation in multicast session services.

The route discovery process of MAODV uses unicast and broadcast mechanisms to transmit control packets. The unicast mechanism of MAODV's route discovery process is targeted by an attacker and the entire route discovery process is disturbed by dropping the unicast control packets at the MAC receiver. Further, the position of the attacker in a multicast tree plays a vital role in this attack. The attacker's success rate is very high only in the following scenarios:

- Multiple branches of a multicast tree are expanded through malicious or suspicious nodes.
- An attacker is a downstream neighbor of a multicast source with a single path connecting the source node with an existing multicast tree.

When an internal suspicious node identifies the presence of a multicast source or receivers within its transmission range, then this node starts to trigger attacks through its MAC layer. In this way, an internal node intelligently executes an attack only when it stands to gain in terms of its attack success rate. The probability that a suspicious node will act maliciously is calculated as follows. The probability of an attacker encountering a multicast-group member ($M$) among a total of $N$ nodes in a network is given by

$$p = \frac{M}{N} = \frac{S+R}{N} = \frac{1+R}{N}, \quad (1)$$

where, $S$ denotes the total number of sources and $R$ the total number of receivers in a multicast group. Here, $S = 1$ and $1 < R \geq N-1$; that is, $M = 1 + R$, where $M \leq N$. The probability of obtaining $k$ consecutive successes from $T$ trials is given by

$$P\ (k > 0) = \frac{T!}{(T-k)!k!} p^k q^{(T-k)}, \quad (2)$$

$$p = \frac{M}{N} P_b, \quad (3)$$

where $k$ represents the number of successes that result from binomial experiments. Here, a "yes/no" experiment is used to indicate whether an attacker's node meets a multicast group member. The total simulation unit time is represented by $T$; the probability of success in each trial is represented by $p$; and $q$ is the probability of failure in each trial ($q = 1 - p$). Here, $P_b$ is the probability of a MAC receiver being busy at the time of receiving a packet.

### 4. Threat Model for Internal Stealthy Attack

Reference [25] introduces a threat modeling concept. A threat model shows an analysis of an existing protocol against a threat profile. A threat tree is an analytical tool that describes the path of an attacker in the case of a particular threat. A threat has an unmitigated component in its attack path from the path's leaf condition to its root. This path is known as a valid path. A valid path of a threat tree indicates a vulnerability of a system. Models of an internal stealthy threat are shown in Figs. 2 and 3 for a MAC source and MAC receiver, respectively. The paths "1.2.1.1.1 – 1.2.1.1 – 1.2.1 – 1.2 – root" in Fig. 2 and "1.1.2.1.1 – 1.1.2.1 – 1.1.2 – 1.1 – root" in Fig. 3 are unmitigated attack paths from the leaf condition in the threat tree to the root. Hence, these valid paths indicate a vulnerability of the IEEE 802.11 MAC protocol.

## IV. Proposed SAMRP Attacker Detection System for Indirect Internal Stealthy Attack in MAODV

In existing stealthy attacker detection systems such as SADEC and BLM, observer nodes utilize a promiscuous mode to collect network layer traffic from their neighbors for intrusion detection. Network layer traffic alone is not enough to

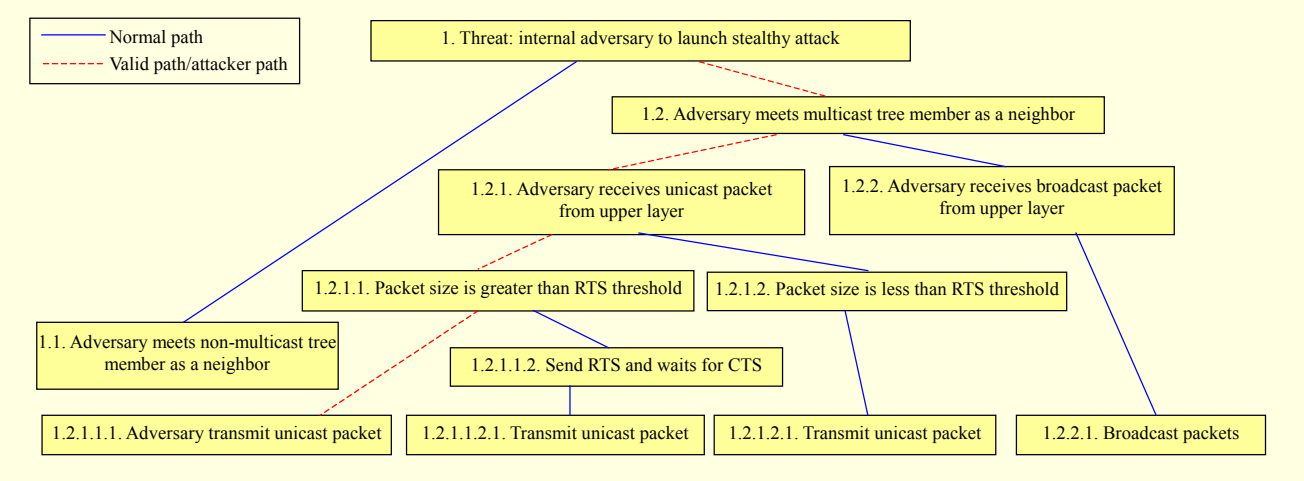



Fig. 2. Threat model for MAC source.

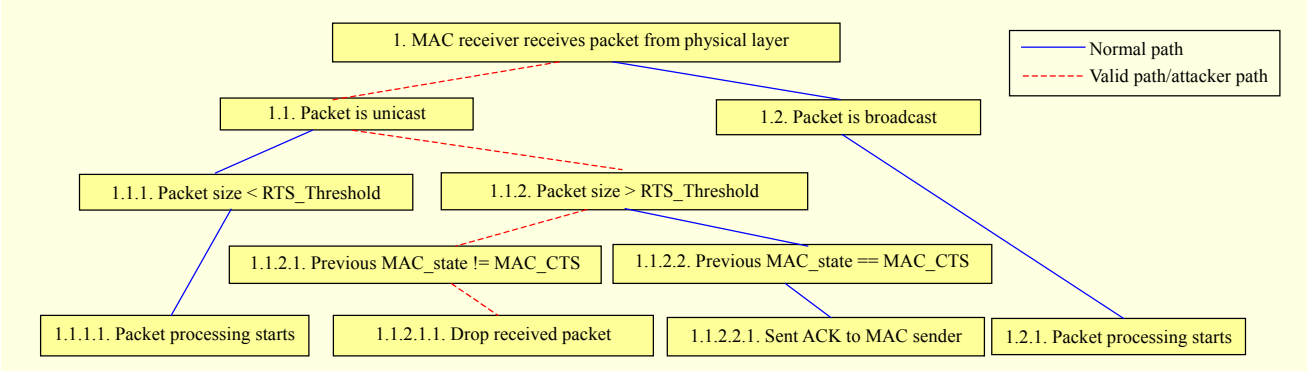



Fig. 3. Threat model for MAC receiver.

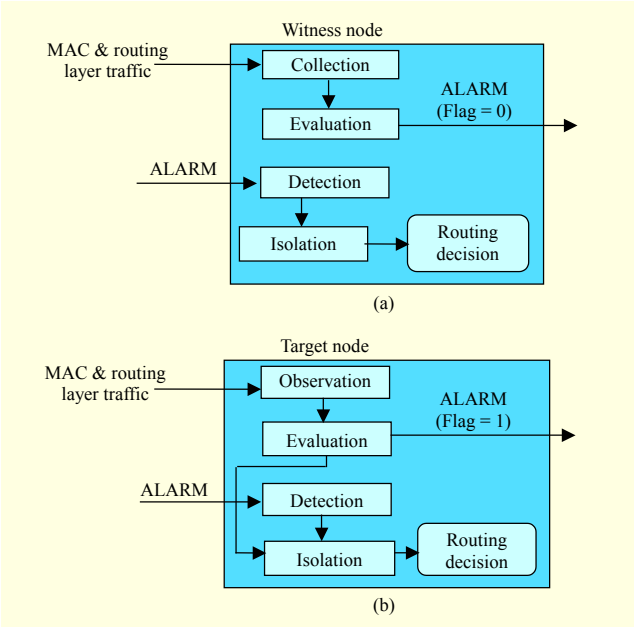



Fig. 4. SAMRP architecture.

identify an indirect internal stealthy attacker. This problem is completely addressed by our novel attacker detection system, SAMRP, for multicast communication environments in MANETs. SAMRP is a combination of a distributed attacker detection and isolation process. The main goals of SAMRP include the identification of malicious nodes and their separation from the normal nodes of a multicast group, and the differentiation of packet drops due to malicious activity or network congestion.

## 1. SAMRP Framework

The SAMRP attacker detection system consists of three major components — *collection* (collect MAC and network traffic logs from local and neighbor nodes), *evaluation* (analyze a collected traffic window to detect misbehavior patterns), and *isolation* (generate and broadcast a warning alarm about an attacker only in positive cases). The architecture of SAMRP is given in Fig. 4. Through promiscuous mode, an observer node can observe its neighbor's communication activities, even if it is not considered as an intended next-hop receiver. If there is a deviation in the collected traffic from the normal traffic log, then the observer node broadcasts an "ALARM" message. Upon receiving the "ALARM" message, a node can add details of the attacker to its blacklist so as to isolate it. The attacker and its legitimate target node are neighbors that can monitor each other's communication behavior. From this point of view, both nodes have the opportunity to blame each other for any unicast packet drops. These observations are carefully analyzed by the SAMRP detection system to identify an actual adversary. In SAMRP, a stealthy attacker's neighbors can be categorized as target nodes; that is, as a MAC-receiver and as a witness node. We improve the SAMRP attacker detection system by incorporating the following features:

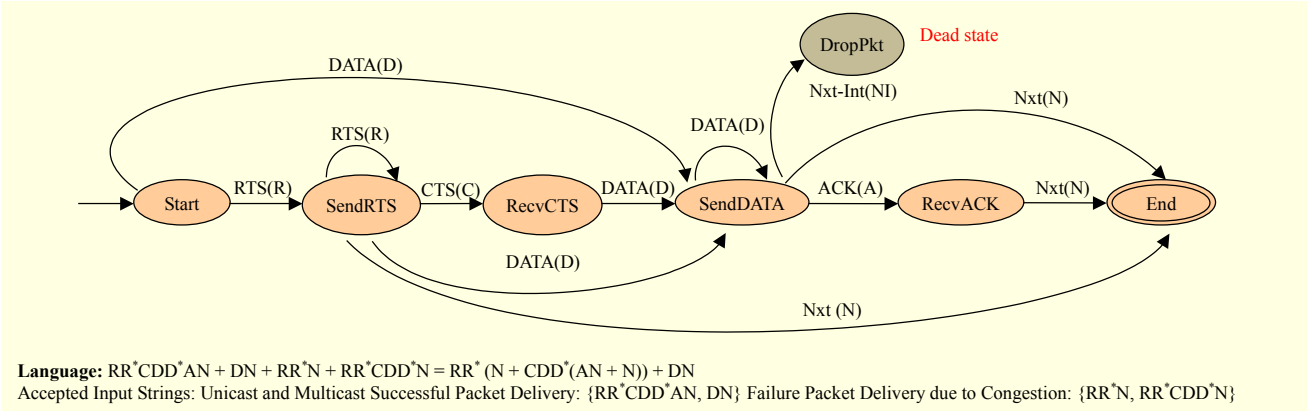
- Collect MAC layer traffic log along with routing layer traffic log.
- Each node triggers SAMRP when it monitors the long-term moderate performance status of a multicast group.
- Collect two different suspect values from an attacker's target and witness nodes.
- Enhanced isolation technique by introducing the total suspect value (TSV) of a suspicious node.

## 2. Traffic Collection

A target node can directly collect and maintain an attacker's MAC and network traffic logs and need not request "promiscuous mode" to observe the actions of its neighbors. From this, a target node can identify an indirect internal stealthy attacker's plan and increase the direct suspect value (DSV) of any suspicious node. However, SAMRP's decision-making system needs an additional supporting suspect value (SSV) from other neighbors of the stealthy attacker; that is, witness nodes. Witness or guard nodes can collect MAC and network traffic logs of the attacker through entering into promiscuous mode. From this enriched cross-layer traffic observation, witness nodes can observe the abnormal patterns such as differences in an attacker's MAC traffic log and frequent unicast control packet drops upon maximum retransmission. Guard nodes may also observe issues in the cases of broadcasting data and control packets.

## 3. Traffic Evaluation

By observing a collected MAC traffic log, guard nodes can differentiate between the probable causes, such as congestion or node misbehavior, of packet drops. We use an automata-based string analysis tool to detect an internal indirect stealthy attacker from a traffic window. This tool accepts or rejects an input string with respect to an internal stealthy attacker's pattern. Each guard node is associated with a non-deterministic finite automata (NFA)–enabled SAMRP architecture. The NFA shown in Fig. 5 represents a set of input strings under an accepted language. A guard node generates a test sequence from observed MAC and network traffic symbols using an adaptive sliding-window concept. Let us assume a sequence in a traffic window to be denoted by Ws. Then, Ws can be used as an input string in an NFA so that the NFA may detect any misbehavior patterns in the string. The NFA is designed to accept a normal cross-layer traffic input string and rejects any




**Language:** RR*CDD*AN + DN + RR*N + RR*CDD*N = RR* (N + CDD*(AN + N)) + DN
Accepted Input Strings: Unicast and Multicast Successful Packet Delivery: {RR*CDD*AN, DN} Failure Packet Delivery due to Congestion: {RR*N, RR*CDD*N}

Fig. 5. NFA-based malicious pattern detection model in traffic window.

| Node ID | Attacker ID | Flag | Sequence No |
|---|---|---|---|

Fig. 6. Format of ALARM message.

string with misbehavior patterns. If any input test sequence in a traffic window is rejected by the NFA, then witness nodes increase their SSV by one for the corresponding suspicious node. When this value reaches a threshold, $\beta$, then the suspicious node is confirmed as an attacker and an "ALARM" message will be broadcast to the entire network to warn of the presence of a stealthy attacker. The threshold $\beta$ is always set to a low value. The "ALARM" packet format is shown in Fig. 6. This packet consists of the following fields: {Node ID, Attacker ID, Flag, Sequence No}.The "Node ID" field represents an observer node; that is, the source of an "ALARM" message. The "Flag" field is composed of the set {0, 1}; that is, 0–DSV and 1–SSV. It indicates an "ALARM" message's observation type; that is, whether it is either a legitimate target node or a witness node of an attacker. The "Sequence No." field shows the *freshness* of the "ALARM" message.

## 4. Distributed Isolation

Each node maintains TSV for identified suspect nodes. TSV values can be calculated only after receiving "ALARM" messages from an attacker's guard and target nodes. TSV is calculated by assigning weight values for two different types of observations with respect to the target and witness nodes, as follows:

$$\mathrm{TSV} = T_A + T_B = \left(\frac{1}{n}\right)\left(\frac{n_1 P_1}{T_R}\right) + \left(\frac{n-1}{n}\right)\left(\frac{n_2 P_2}{T_R}\right), \quad (4)$$

$$\mathrm{TSV} = \begin{cases} T_A + T_B & T_A > 0 \text{ and } T_B > 0, \\ 0 & \text{Else}. \end{cases} \quad (5)$$

Consider the total number of "ALARM" packets received by a node to be $T_R$. Then, $T_R = T_A + T_B$, where $T_A$ and $T_B$ represent the number of "ALARM" packets sent by the target node (Flag = 1) and witness nodes (Flag = 0) of the attacker, respectively. Furthermore, $n = n_1 + n_2$, where $n$ represents the total number of nodes, including the target node ($n_1$) and witness nodes ($n_2$) of an attacker from which the "ALARM" packets are received by the node.

$$T_A = n_1 P_1, \quad T_B = n_2 P_2, \quad (6)$$

where $n_1$ represents the number of target nodes from which "ALARM" packets are received for a particular suspect node. Here, $n_1$ is set to a value of "1" based on the assumption that an internal stealthy attacker targets a single node at a time for unicast communications. In (6), $P_1$ represents the number of packets received under DSV; that is, from a target node; $P_2$ represents the number of "ALARM" packets received from individual guard nodes; and $n_2$ represents the number of witness nodes from which "ALARM" packets were received. Hence, (6) can be rewritten as

$$T_A = P_1 T_B = n_2 P_2. \quad (7)$$

TSV is calculated by adding two different observations, SSV and DSV, only when $T_A$ and $T_B$ are both greater than zero. The TSV calculation method shows that if any one of the observations is missing, then TSV is set to 0. A decision about a suspicious node is taken only after considering the observations from both the target node and the witness nodes. Each node, via its suspect values, maintains a blacklist of nodes that are suspected as belonging to an internal stealthy attacker. If the TSV of a suspicious node reaches a threshold value, $\beta_1$, then the node's details are added to the blacklist of the node calculating the TSV by setting the corresponding suspect node's "Flag" field value to "1." Each node evades the blacklist nodes from its multicast service.

Nodes in an SAMRP environment also maintain a *suspect table* to facilitate a security feature in multicast communication

| Suspect Node ID | DSV | SSV | TSV | Blacklist Flag | Time |
|---|---|---|---|---|---|
| A | 0.1 | 0.45 | 0.55 | 1 | 36.8210 |

Fig. 7. Structure of suspect table.

shown in Fig. 7. The fields of such a suspect table are as follows: {Suspect Node ID, DSV, SSV, TSV, Blacklist Flag, Time}. The "Blacklist Flag" field is set to either "0" (not yet confirmed as an attacker) or "1" (confirmed as an attacker).

This field is initialized to "0" for newly added entries. A suspect table is updated whenever a node receives "ALARM" packets from either guard or witness nodes. Furthermore, a unique record is maintained for each suspect node, and such a table will maintain a list of blacklisted nodes found to be in a multicast group. When a node receives an "ALARM" packet, it checks the status of any corresponding suspicious nodes recorded in its suspect table. If it is the first "ALARM" message received about a particular suspicious node, then a new record is added to the suspect table. If a record already exists in the table, then the entries in the DSV, SSV, and Time fields are updated.

We can calculate the TSV value of a node using (4) and (5). If a node's TSV value exceeds a threshold value, then the "Blacklist Flag" field is set to "1," indicating that a suspicious node is confirmed as an indirect internal stealthy attacker. The "Time" field indicates the time when an "ALARM" packet reached a node, showing the *freshness* of a record.

## V. Theoretical Analysis

### 1. Throughput

We modify the analytical model proposed by Bianchi [26] to determine the maximum achievable saturation throughput with respect to an internal stealthy attacker. The Bianchi throughput model considers the average time of a channel sensed busy only under a successful transmission and collision circumstances. We use the assumptions and parameters of the Bianchi model for our own theoretical analysis. Some of these assumptions are as follows: $n$ is the number of stations contending for channel access. We assume that a packet collision occurs only in an RTS frame from the perspective of the attacker. In an internal stealthy attack, a payload packet may be dropped by the receiver due to its busy state. If so, then the packet is retransmitted for a permitted maximum number of times. A normalized system throughput, $S$, is calculated as follows for the RTS/CTS mechanism. As per the Bianchi model, $P_{tr}$ denotes the probability that at least one transmission occurs within a given slot time; $\tau$ is each station's packet transmission probability. The probability that a successful transmission occurs on a channel is denoted by $P_s$. Hence, $P_s$ and $P_{tr}$ are calculated using the following formulae [26]:

Table 1. Throughput obtained from analytical model.

| RTS/CTS access | | |
|---|---|---|
| $N$ | Max. throughput approximation (Normal) | Max. throughput approximation (with attacker) |
| 5 | 0.838436 ($\tau$ = 0.097940) | 0.803696 ($\tau$ = 0.029601) |
| 10 | 0.837129 ($\tau$ = 0.048970) | 0.800616 ($\tau$ = 0.014800) |
| 20 | 0.836490 ($\tau$ = 0.024485) | 0.799095 ($\tau$ = 0.007400) |
| 50 | 0.836160 ($\tau$ = 0.009794) | 0.798188 ($\tau$ = 0.002960) |
| $\infty$ | 0.835859 ($K$ = 2.042) | 0.798096 ($K$ = 6.756) |

$$P_{tr} = 1-(1-\tau)^n, \tag{8}$$

$$P_s = \frac{n\tau(1-\tau)^{n-1}}{P_{tr}} = \frac{n\tau(1-\tau)^{n-1}}{1-(1-\tau)^n}. \tag{9}$$

The average time a channel is sensed busy due to a successful packet transmission is denoted by $T_s$. The average channel busy time due to a collision in a considered time slot (from the Bianchi model [26]) is denoted by $T_c$.

$$T_s^{RTS} = \text{RTS} + \text{SIFS} + \delta + \text{CTS} + \text{SIFS} + \delta + H + \text{E[P]} + \text{SIFS} + \delta + \text{ACK} + \text{DIFS} + \delta,$$

$$T_c^{RTS} = \text{RTS} + \text{DIFS} + \delta.$$

The payload size is E[$P$]. Here, $P_{tr}P_s$E[$P$] represents the average payload size successfully transmitted in a given slot time. A collision in a timeslot is denoted by $P_{tr}(1–P_s)$. Then, the throughput is calculated in the Bianchi model [26] as follows:

$$S = \frac{\text{E}[P]}{T_s - T_c + \dfrac{\sigma(1-P_{tr})/P_{tr} + T_c}{P_s}}. \tag{10}$$

We include the time the channel is sensed busy due to the unicast packets dropped by an internal stealthy attack.

$$T_A^{RTS} = H + \text{E}[P^*] + \text{DIFS} + \delta, \tag{11}$$

where E[$P$], $T_s$, $T_c$, $T_A$, and $\sigma$ are all expressed in the same unit. Then, the maximum achievable throughput, $S$, under an internal stealthy attack is calculated using

$$S_{(a)} = \frac{\text{E}[P]P_sP_{tr}}{(1-P_{tr})\sigma + P_{tr}P_sT_s + \dfrac{P_{tr}(1-P_{tr})(T_c+T_A)}{2}},$$

$$S_{(a)} = \frac{2\text{E}[P]}{2T_s - (T_c+T_A) + \dfrac{2\sigma(1-P_{tr})/P_{tr} + (T_c+T_A)}{P_s}}, \tag{12}$$

$$T_A^* = \frac{T_c+T_A}{2\sigma}, \qquad \tau = \frac{1}{n\sqrt{T_A^*/2}}.$$

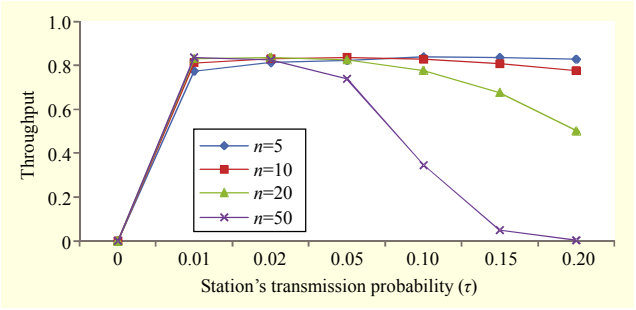



Fig. 8. Throughput without attacker.

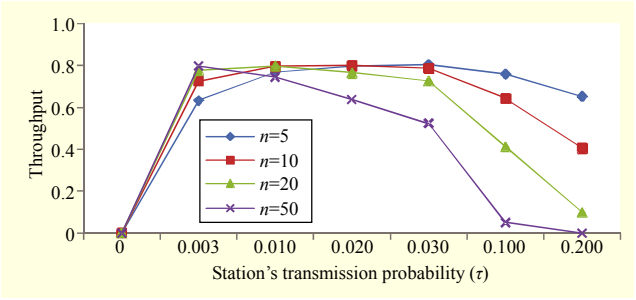



Fig. 9. Throughput with internal stealthy attacker.

The maximum achievable throughput, $S_{max}$, can be calculated with respect to the number of independent contending stations within the network. Let us suppose that $n$ takes on a very large value, then the throughput calculation can be modified as follows. Calculate $K$ using $\sqrt{T_c^*/2}$ and $K = 2.042$ for the RTS/CTS mechanism. Then, $P_{tr}$ and $P_s$ are rearranged as follows using $K$:

$$P_{tr} = 1-(1-\tau)^n = 1-\left(1-\frac{1}{nK}\right)^n \approx 1-e^{-1/K},$$

$$P_s = \frac{n\tau(1-\tau)^{n-1}}{P_{tr}} \approx \frac{1}{K(e^{1/K}-1)}.$$

Then, $S_{max}$ is rearranged based on the modified $P_{tr}$ and $P_s$ as follows:

$$S_{max} = \frac{E[P]}{T_s + \sigma K + T_c\left(K(e^{1/K}-1)-1\right)}. \quad (13)$$

With an attacker in RTS/CTS access mode, $K$ is calculated from $\sqrt{T_A^*/2}$. Then, $K = 6.756$. Correspondingly, the maximum saturation achievable throughput under a stealthy attacker, $S_{max(a)}$, can be calculated using the following formula:

$$S_{max(a)} = \frac{E[P]}{T_s + \sigma K + \frac{(T_c+T_A)\left(K(e^{1/K}-1)-1\right)}{2}}. \quad (14)$$

For comparison purposes, we use the same parameters used by Bianchi [26] to evaluate our analytical model. Parameter values used for the analytical model are given in [26]. The results shown in Table 1, Fig. 8, and Fig. 9 are obtained from (12) by considering the presence and non-presence of an internal stealthy attacker in the network.

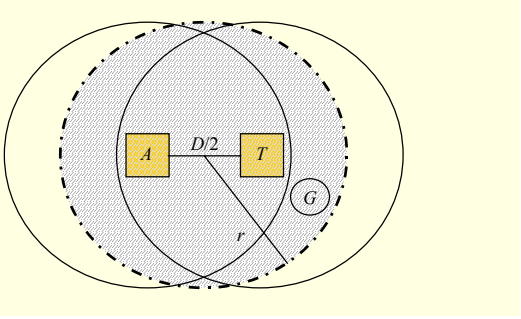



Fig. 10. Indirect internal stealthy attacker scenario with guard node.

## 2. SAMRP vs. SADEC

This subsection analyzes the internal-stealthy-attacker detection probability of SAMRP and SADEC under different multicast group scenarios. We adapted the theoretical model proposed by Khalil and Bagchi [13] for SADEC for use with our proposed system. We use the same assumptions and parameters of the Khalil model. We validate the accuracy of SAMRP with SADEC through attacker isolation probability using theoretical analysis. Consider two neighbor nodes; Node $A$ is the stealthy attacker and node $T$ is the target node. Node $T$ drops a unicast packet sent by node $A$ if node $T$ has failed to send an RTS packet to Node $A$ immediately beforehand. Nodes $T$ and $A$ are separated by distance $D$, and the transmission range in between them is denoted by $r$. A guard region is calculated, as in Fig. 10. The nodes in the shaded region will act as guard nodes ($G$). The guard region ensures that a selected guard node ($G$) is a common neighbor to both node $A$ and node $T$. Our proposed model extends the Khalil model [13] with respect to an additional MAC layer traffic log. Node $A$ sends an RTS with probability $P_{rts}$ and DATA packet with probability $P_{data}$. Node $T$ has probability $P_{cts}$ of sending a CTS frame and $P_{ack}$ of sending an ACK frame. RTS, CTS, and ACK frames are accounted for and interpreted only by the SAMRP architecture–enabled guard nodes. Whereas, SADEC can interpret only "$DATA_{in}$" and "$DATA_{out}$" packets from nodes $A$ and $T$. Thus, SAMRP has the following different possibilities:

- $G$ obtains RTS and CTS packets from nodes $A$ and $T$, respectively.
- $G$ obtains $DATA_{in}$ and $DATA_{out}$ packets from nodes $A$ and $T$, respectively.
- $G$ obtains an ACK packet from node $T$.

Node $A$ relays an RTS frame and $T$ responds with a CTS

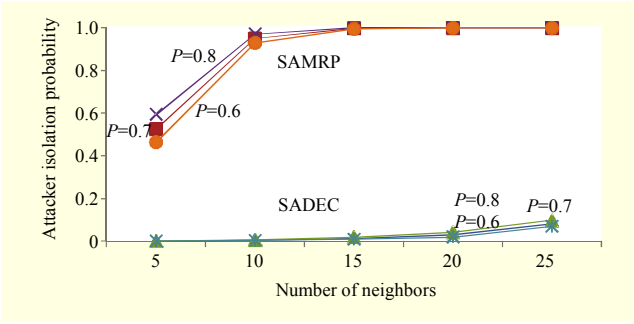



Fig. 11. Probability of attacker isolation of SAMRP and SADEC with different attacker detection probability.

packet. Then, node $A$ sends $DATA_{in}$ and node $T$ forwards $DATA_{out}$ to its neighbors. Also, node $T$ sends an ACK packet only when a data packet has successfully reached it.

The following assumptions are adapted from the Khalil model [13]: $P_c$ is the probability of a missing packet due to channel error; $P_c$ is a negligible value (that is, 0.01); $\mu$ is the number of data packets dropped by node $T$ within a traffic window ($T_{win}$); $\mu = \Psi * P_{mal} * (1–P_c)$; $\Psi$ is the number of data packets sent by node $A$ with $T_{win}$ to node $T$. The probability of SAMRP is calculated as follows:

$$P_{rts/cts} = P_{rts}P_{cts} = (1-P_c)(1-P_c) = (1-P_c)^2,$$
$$P_{Data/Ack} = P_{in}P_{out}P_{ack} = (1-P_c)^3.$$

According to the traffic of a MAC layer, SADEC cannot interpret RTS, CTS, and ACK packets for an attacker detection mechanism. So, these packets are treated as missing by guard node $G$. Hence, the probabilities for a guard node in SADEC are as follows:

$$\begin{aligned} P_{rts/cts} &= P_{rts}P_{cts} = P_c\,P_c = (P_c)^2, \\ P_{Data/Ack} &= P_{in}P_{out}P_{Ack} = (1-P_c)^2 P_c, \\ P_{1\&2} &= (P_{rts/cts} + P_{Data/Ack})/2. \end{aligned} \quad (15)$$

The attacker detection and isolation functions are adapted from the Khalil model as follows:

$$P_{detect} = \sum_{i=\beta}^{\mu} \binom{\mu}{i} (P_{1\&2})^i (1-P_{1\&2})^{\mu-i}, \quad (16)$$

$$P_{detect} = \sum_{i=\beta}^{\mu} \binom{\mu}{i} (P_{1\&2})^i (1-P_{1\&2})^{\mu-i}. \quad (17)$$

This theoretical model gives a better performance in the case of the SAMRP attacker detection system over the existing SADEC against an internal stealthy attack (see Fig. 11).

## VI. Simulation Results

In this section, we discuss the effectiveness of an indirect internal stealthy attack on MAODV and evaluate the performance of SAMRP using NS-2 simulation results.

### 1. Performance Metrics

The following performance metrics along with packet delivery ratio (PDR) and multicast throughput are used to analyze the impact of an attacker on MAODV:

- *Attacker's Degree of Source Node:* fraction of attackers in the transmission range of the multicast source over its neighbors.
- *Multicast Receiver's Degree of Attacker (with respect to Total Neighbors):* number of receivers in the transmission range of an attacker over the degree of attacker.
- *Attacker's Vicinity (with respect to Total Receivers in the Multicast Group):* Ratio between the number of multicast receivers in attacker's transmission range and the total number of receivers in the multicast group.

To evaluate the performance of the SAMRP detection system on MAODV, we use the following performance metrics:

- *Attacker Isolation Probability*: fraction of number of isolated internal stealthy attackers over the total number of stealthy attackers in the network.
- *Percentage of False Isolation*: fraction of legitimate nodes isolated as an attacker over the total number of legitimate nodes.

### 2. Simulation Environment

Simulations are performed using a discrete event network simulator NS 2.35 [27] to analyze the behavior of the MAODV [13], [28] multicast routing protocol against an internal stealthy attack. The simulation area is set to 1,800 m × 1,800 m. In total, 25 nodes are randomly placed within the simulation area. Each simulation runs for 300 s. The nodes use a 2 Mbps data transmission rate and have a 250 m transmission range. The source sets the multicast data packet rate at 512 bytes per second. IEEE 802.11 is a MAC layer protocol, and MAODV is a network layer protocol, respectively for multicast communication. Each simulation is run ten times so as to be able to calculate an average value for each performance metric. The multicast group is defined as {5, 10, 15, and 18} and is used for different experimentations. Each node follows a random-waypoint mobility model. Attacker nodes are randomly chosen, either from the multicast tree or group members, with attackers being linearly introduced in the multicast tree.

### 3. Effect of Stealthy Attack on MAODV

Figure 12(a) shows the impact of a stealthy attack on the PDR of MAODV, with the number of attackers set from 0 to 3.

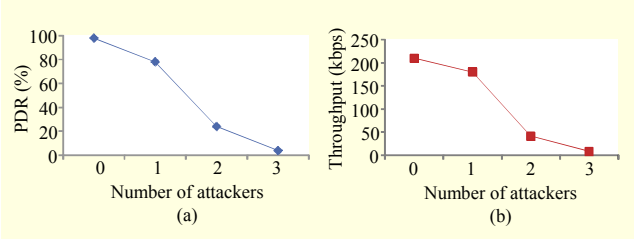



Fig. 12. Impact of internal stealthy attacker on: (a) PDR and (b) throughput of MAODV.

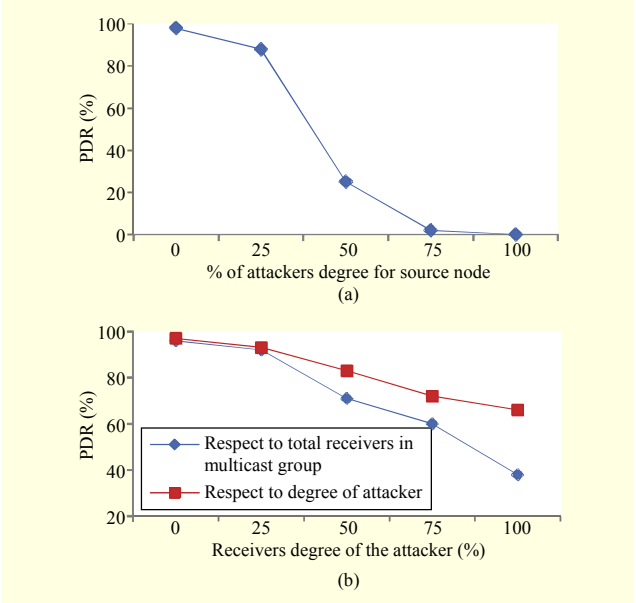



Fig. 13. Impact of attacker's location: (a) near to multicast source and (b) near to multicast receiver.

MAODV can maintain its PDR at nearly 80% when a single attacker is present in the network. However, MAODV struggles to maintain its PDR when a further two attackers are introduced into the environment. A significant degradation of PDR is induced by three attackers in the multicast group. Figure 12(b) shows MAODV's multicast throughput variation against a number of internal stealthy attackers. The throughput decline ratio is nominal; that is, 12% at the time a single attacker is active in the multicast group. Then, a sudden decline in the throughput is explained by the fact that more than one stealthy attacker is having a major impact on MAODV. A maximum of three attackers can decrease the multicast throughput to less than 40 kbps.

Figure 13(a) explains an attacker's impact on PDR with respect to the degree of multicast sources when attackers exist in its transmission range. If a multicast source has a single path to connect all multicast receivers and this neighbor is an attacker, then the entire multicast tree is harmed. MAODV gives a PDR of nearly 0% in such a case. Even if 50% of the multicast source's neighbors are set as an attacker, then a major decline in PDR occurs. A drop in PDR can be reduced by increasing the degree of multicast sources.

Figure 13(b) shows the effect of a stealthy attack on PDR with respect to the percentage of multicast receivers in the attacker's transmission range. Simulation results show that the PDR slowly decreases to 62% when an attacker has more multicast receivers in its transmission range. If an attacker's neighbors are all multicast receivers, then the PDR difference ratio differs by up to 35% from the initial PDR. If the attacker has a single multicast receiver in its transmission vicinity, then the PDR difference ratio is very small; that is, only 5%. Figure 13(b) shows the effect of a stealthy attack on PDR with respect to the percentage of multicast receivers in the transmission range of an attacker over the total number of receivers in the multicast group. If 25% of receivers in the multicast group are an attacker's neighbors, then the PDR difference ratio is significantly small; that is, only 2% from its initial PDR. If all the receivers of the multicast group are located within the transmission range of the attacker, then the PDR drops to 30%.

## 4. Performance Evaluation of SAMRP Detection Technique

Figure 14 shows the attacker isolation probability of SAMRP against the number of attackers in a network. We compare the SAMRP with BLM and SADEC, existing attacker detection systems to evaluate the performance of our proposed system. Simulation results show that the SAMRP's attacker isolation probability is higher than that of BLM and SADEC. Existing systems misconclude the internal stealthy attacker as a legitimate node and falsely isolate a legitimate node as the packet-drop attacker from the observed network layer traffic logs collected by the observer. BLM and SADEC can not interpret the MAC layer packets to detect a stealthy attacker's behavior. Figure 16 shows that the attacker isolation probability of SAMRP is higher than 0.9 when the number of attackers is not given any consideration. At the same time, BLM and SADEC give an attacker's isolation probability of less than 0.1. Figure 15 shows the false-isolation probabilities

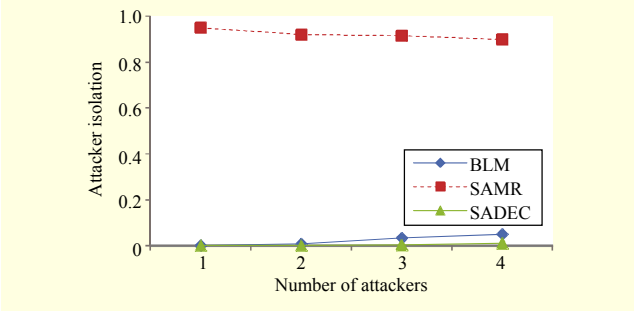



Fig. 14. Attacker isolation probability vs. number of attackers.

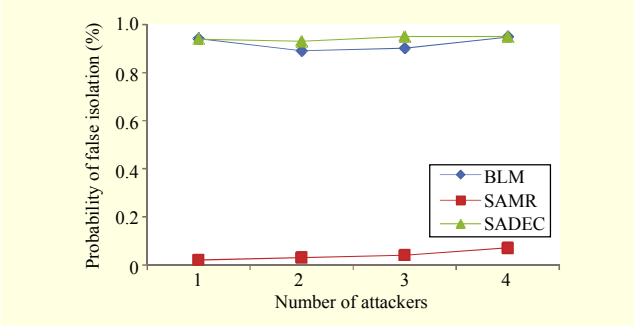



Fig. 15. Probability of false isolation vs. number of attackers.

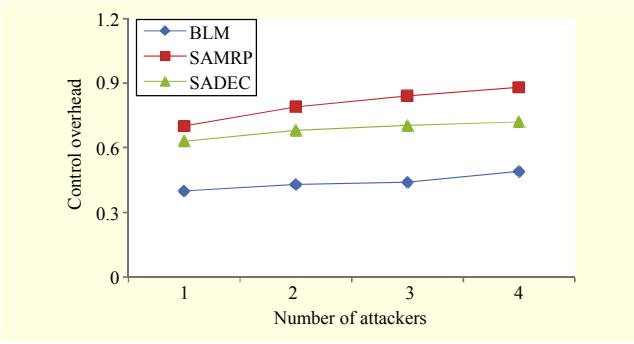



Fig. 16. Control overhead vs. number of attackers.

of attacker detection systems SAMRP, SADEC, and BLM in a multi cast environment. The probability of false isolation in the cases of BLM and SADEC increases by increasing the number of attackers.

Figure 16 shows the control overheads induced by a stealthy attacker for detection systems such as BLM, SADEC, and SAMRP. The control overhead of SAMRP is higher than that of BLM and SADEC. The control overhead of SAMRP is induced by the additional warning control packet "ALARM" in MAODV. The control overhead of a detection system increases with an increased number of attackers. It shows that the number of "ALARM" messages generated by a guard node increases with the number of attackers.

## VII. Conclusion

In this paper we have introduced a novel indirect internal stealthy attack with the intent to disrupt the multicast services of a MANET. This is achieved by exploiting an RTS/CTS mechanism to target the unicast control packets of the multicast route discovery process; such behavior cannot be detected by existing intrusion detection systems such as SADEC and BLM. Through simulation and analytical results, we have proved that the SADEC detection system fails to detect an attacker node and falsely accuses a legitimate node of being a malicious node. Hence, we have proposed an SAMRP detection system for an indirect internal stealthy attack. Our system can successfully detect and isolate a stealthy attack from a multicast group. Our automata-based attacker detection system is designed to observe MAC and routing layer traffic logs and analyze malicious patterns in traffic windows. Simulation and analytical results show that SAMRP gives better performance when compared to the BLM and SADEC detection systems against an indirect internal stealthy attack on a multicast communication in MANETs.

## References

[1] K. Obraczka and G. Tsuiuk, "Multicast Routing Issues in Ad Hoc Networks," *IEEE Int. Conf. Universal Pers. Commun.*, Florence, Italy, vol. 1, Oct. 5–9, 1998, pp. 751–756.

[2] H.L. Nguyen and U.T. Nguyen, "A Study of Different Attacks on Multicast in Mobile Ad Hoc Networks," *Ad Hoc Netw.*, vol. 6, no. 1, Jan. 2008, pp. 32–46.

[3] J. Dong, R. Curtmola, and C.N. Rotaru, "Secure High-Throughput Multicast Routing in Wireless Mesh Networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 5, 2011, pp. 653–668.

[4] R. Curtmola and C.N. Rotaru, "BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-hop Wireless Networks," *IEEE Trans. Mobile Comput.*, vol. 8, no. 4, 2009, pp. 445–459.

[5] A.M.A. Mo'men, H.S. Hamza, and I.A. Saroit, "New Attacks and Efficient Countermeasures for Multicast AODV," *HONET*, Cairo, Egypt, Dec. 19–21, 2010, pp. 51–57.

[6] A.M.A. Mo'men, H.S. Hamza, and I.A. Saroit, "A Survey on Security Enhanced Multicast Routing Protocols in Mobile Ad Hoc Networks," *HONET*, Cairo, Egypt, 2010, pp. 262–268.

[7] F. He, K. Hao, and H. Ma, "S-MAODV: A Trust Key Computing Based Secure Multicast Ad Hoc on Demand Vector Routing Protocol," *IEEE ICCSIT*, Chengdu, China, vol. 6, July 9–11, 2010, pp. 434–438.

[8] S. Roy et al., "Securing MAODV: Attacks and Countermeasures," *IEEE SECON*, Santa Clara, CA, USA, Sept. 2005, pp. 521–532.

[9] A.A. Mo'men, H.S. Hamza, and I.A. Saroit, "Secure Multicast Routing Protocols in Mobile Ad-Hoc Networks," *Int. J. Commun. Syst.*, vol. 27, no. 11, Nov. 2014, pp. 2808–2831.

[10] A.M. Pushpa and K. Kathiravan, "Secure Multicast Routing Protocol against Internal Attacks in Mobile Ad Hoc Networks," *IEEE GCC*, Doha, Qatar, Nov. 17–20, 2013, pp. 245–250.

[11] A.M. Pushpa and K. Kathiravan, "Resilient PUMA (Protocol for Unified Multicasting through Announcement) against Internal Attacks in Mobile Ad Hoc Networks," *ICACCI*, Mysore, India, Aug. 22–25, 2013, pp. 1906–1912.

[12] I. Khalil and S. Bagchi, "Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure," *IEEE Trans. Mobile Comput.*, vol. 10, no. 8, Aug. 2011, pp. 1096–1112.

[13] E. Royer and C. Perkins, "Multicast Ad-Hoc on-Demand

Distance Vector (MAODV) Routing," Internet Draft, July 2000.
[14] A.M. Pushpa and K. Kathiravan, "Intelligent Stealthy Attack on MAODV in Mobile Ad Hoc Networks," *Int. Conf. Adv. Comput.*, Chennai, India, Dec. 17–19, 2014, pp.1–6.
[15] P. Mohapatra, C. Gui, and J. Li, "Group Communications in Mobile Ad Hoc Networks," *Comput.*, vol. 37, no. 2, Feb. 2004, pp. 52–59.
[16] H. Gossain et al., "Supporting MAC Layer Multicast in IEEE 802.11-Based MANETs: Issues and Solutions," *IEEE Int. Conf. Local Comput. Netw.*, Tampa, FL, USA, Nov. 2004, pp. 172–179.
[17] S. Kumar, V.S. Raghavan, and J. Deng, "Medium Access Control Protocols for Ad Hoc Wireless Networks: A Survey," *Ad Hoc Netw.*, vol. 4, no. 3, May 2006, pp. 326–358.
[18] E.M. Royer, S.J. Lee, and C.E. Perkins, "The Effects of MAC Protocols on Ad Hoc Network Communication," *IEEE WCNC*, Chicago, IL, USA, vol. 2, 2000, pp. 543–548.
[19] Q. Chen et al., "Overhaul of IEEE 802.11 Modeling and Simulation in NS-2," *MSWiM*, Chania, Greece, 2007, pp. 159–168.
[20] L.K. Law, S.V. Krishnamurthy, and M. Faloutsos, "Understanding and Exploiting the Trade-Offs between Broadcasting and Multicasting in Mobile Ad Hoc Networks," *IEEE Trans. Mobile Comput.*, vol. 6, no. 3, 2007, pp. 264–279.
[21] F.S. Wattenberg et al., "Anomaly Detection in Network Traffic Based on Statistical Inference and α-Stable Modeling," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 4, July-Aug. 2011, pp. 494–509.
[22] C. O'Reilly et al., "Anomaly Detection in Wireless Sensor Networks in a Non-stationary Environment," *IEEE Commun. Surveys Tutorials*, vol. 16, no. 3, 2014, pp. 1413–1432.
[23] S. Misra et al., "LAID: A Learning Automata-Based Scheme for Intrusion Detection in Wireless Sensor Networks," *Security Commun. Netw.*, vol. 2, no. 2, 2009, pp. 105–115.
[24] F. Yu et al., "Automata-Based Symbolic String Analysis for Vulnerability Detection," *Formal Methods Syst. Des.*, vol. 44, no. 1, Feb. 2014, pp. 44–70.
[25] F. Swiderskia and W. Snyder, "*Threat Modeling (Microsoft Professionals)*," Microsoft Press, 1st Edition, 2004, pp. 1–240.
[26] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, Mar. 2000, pp. 535–547.
[27] *The Network Simulator - NS2*. Accessed Oct. 1, 2015. http://www.isi.edu/nsnam/ns/
[28] Y. Zhu and J. Kunz, "MAODV Implementation for NS 2.26," Carleton University, Technical Report, SCE–04–01.

**Menaka Pushpa Arthur** is a PhD student with the Department of Computer Science and Engineering, Easwari Engineering College, Anna University, Chennai, India. She received her ME degree in computer science and engineering from Anna University, India and her BE degree in computer science and engineering from Madurai Kamaraj University, India, in 2004 and 2002, respectively. She is a lifetime member of the Indian Society for Technical Education. Her research focuses on mobile ad hoc networks, multicast routing, security attacks, and intrusion detection systems.

**Kathiravan Kannan** received his MTech degree in electronics and communication engineering from Pandicherry University, India and his PhD degree in mobile ad hoc networks from Anna University, Chennai, India, in 2001 and 2007, respectively. He is currently the dean of Easwari Engineering College, Chennai, India. He was the project coordinator for two All India Council for Technical Education funded research projects. He has nearly 20 years of teaching experience in various reputed institutions in India. This year, he is to perform the role of convenor at the IEEE International Conference on Technological Innovations in ICT for Agriculture and Rural Development, 2015. He is a lifetime member of the IEEE, Institution of Engineering and Technology, and Indian Society for Technical Education. His main research interests include mobile ad hoc networks, wireless sensor networks, unmanned aerial vehicles, and robotics.