Colluding Injected Attack in Mobile Ad-hoc Networks

Farah Kandah*, Yashaswi Singh*, Chonggang Wang†
Department of Computer Science, North Dakota State University, Fargo, ND 58105*
NEC Laboratories America, Princeton, NJ 08536†

***Abstract*—The growth of laptops, personal digital assistant (PDA) and 802.11/Wi-Fi wireless networking have made mobile ad-hoc network (MANET) and machine-to-machine (M2M) popular research topics recently. With more attention on M2M and MANETs lately, the security issues become more important and urgent for managing and deploying in such networks. The flexible deployment nature and the lack of fixed infrastructure make MANETs suffer from varieties of security attacks. In this paper, we show how an adversary can utilize a colluding attack in MANET by injecting malicious nodes in the network, while hiding their identities from other legitimate nodes. We will name this attack as the Colluding Injected Attack (CIA). These injected nodes will work together to generate a severe attack in the network, which aims to create a collision at an arbitrary node, which in turn will result in making the attacked node unable to receive or relay any packet. As a result this node could be wrongly reported as having a malicious behavior by any other node in the same neighborhood, or it might be reported as unreachable if it is a destination node. Our simulation results show that the existence of an adversary that launching the colluding injected attack (CIA) will mislead the decision of previous attack detection schemes.**

Keywords: Mobile ad-hoc networks, adversary, malicious, colluding, attack.

I. Introduction

Machine-to-Machine (M2M) refers to the technologies that allow the communication between both wireless (*stationary or mobile*) and wired systems with other devices of the same ability [19]. Modern M2M communication has expanded to cover a system of networks that transmits data to personal appliances. Information technology and its rapid development made M2M become an indispensable part of our life, such as water and electricity automatic meter, smart home, parking service, vending machines and so on [2] [15] [19] [23]. Machines in these businesses include control equipment, data collector equipment, data manager equipment and data transfer equipment and so on. M2M creates a digital world which is more convenient to people. Different technologies and applications of M2M refer to five important parts: M2M hardware, machines, middleware, communication networks, and applications. Communication networks are the core position in the entire M2M technology framework [19], which include wireless communication network, satellite communication network, Internet, wireless local area networks (WLAN), Bluetooth, wireless personal area network (WPAN), sensor network and so on.

Ad-hoc networks are multihop wireless networks consisting of a large number of wireless radio equipped nodes that may be as simple as *stationary* nodes to *mobile* portable laptops mounted on vehicles or carried by people [17]. Mobile ad-hoc network (MANET) is a self configuring network of mobile devices connected by wireless links, where each device can change its links to other devices frequently, due to its ability to move independently in any direction [18]. An example of mobile ad-hoc network is shown in Fig. 1.

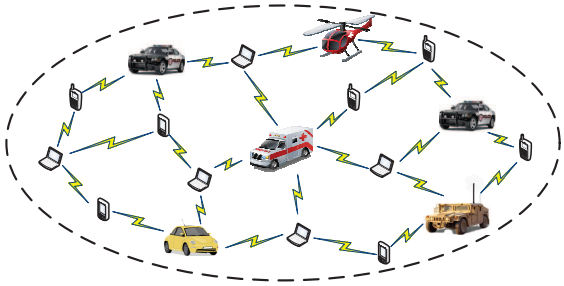

Fig. 1. Mobile ad-hoc network example

The growth of laptops, personal digital assistant (PDA) and 802.11/WiFi wireless networking have made MANETs a popular research topic recently. MANETs have attracted many research to evaluate protocols and abilities of existing protocols in such networks with the existence of mobility. Different evaluated works have been made based on the packet drop rate, the overhead introduced by the routing protocol, energy consumption in [11] [17]. This growth in wireless networks recently has made it far easier for M2M communication to take place, where it reduced the amount of power and time needed for information to be transmitted between machines [2] [15].

With more attention on M2M and MANETs lately, the security issues become more important and urgent for managing and deploying in such networks. The *flexible deployment nature* and the *lack of fixed infrastructure* make MANETs suffer from varieties of security attacks [6], where the existence of such attacks might hold back the growth of this promising wireless network technology.

In this paper, we show how an adversary can utilize the use of multiple nodes to create a colluding attack in MANET. Where an adversary will inject a full controllable powerful malicious nodes in the network, while hiding their identities from other legitimate nodes in the network. We will name this attack as the **C**olluding **I**njected **A**ttack (**CIA**). These injected nodes will work together to generate a severe attack in the network, which aims to prevent a specific node from receiving any packet. This proposed attack will make use of the hidden terminal problem

978-1-4244-9920-5/11/$26.00 ©2011 IEEE

and create a collision at an arbitrary node, which in turn will result in making the attacked node unable to receive or relay any packet. Also the CIA attack in a neighborhood aims to mislead the watchdogs nodes (*nodes that used to monitor the behavious of other nodes in a neighborhood*) in wrongly reporting the attacked node (*the legitimate node*) as behaving maliciously in this neighborhood. In this work, we show that previously proposed detection schemes are unable to mitigate the effect or detect our proposed colluding injected attack (CIA) in MANET.

The rest of this paper is organized as follows. The related work is discussed in Section II. Our models and motivations are discussed in Section III. Our **C**olluding **I**njected **A**ttack (**CIA**) is presented in Section IV, which is followed by the numerical results in Section V. We conclude the paper in Section VI.

II. Related work

Recent studies and researches have shown that security attacks are holding back the potential advantages and wide-scale deployment of wireless networks technology [5]. Due to the wireless nature of wireless ad-hoc networks, if a node is transmitting a packet, all the other nodes in its transmission range (neighboring nodes) will receive its packet and sense that this node is sending. Here these nodes can be assigned as watchdog nodes to monitor the behavior of the transmitting node. The watchdog method has been studied in multiple research for detecting misbehaving nodes in a specific neighborhood, to see if there exists any node in a neighborhood that is not relaying the packets that are not designated to it.

Mari *et al.* in [13] studies some techniques for improving the throughput in mobile ad-hoc networks in the presence of nodes that agree to forward packets but fail to do so. In their work they categorizing nodes as *watchdog nodes* that identifies misbehaving nodes and *pathrater nodes* that helps routing protocols avoiding these nodes. The watchdog technique has some advantages in its ability to detect misbehaving nodes in a static non colluding neighborhood, while its weaknesses are that it might not detect a misbehaving node in the presence of an ambiguous collisions, receiver collisions, limited transmission power, false misbehavior, collusion, and partial dropping [13].

Basic local monitoring (BLM) [10] has been demonstrated to be a powerful technique in detecting misbehaving nodes in multi-hop ad-hoc networks. In BLM, guarding nodes (*watchdog nodes*) are able to monitor other nodes for misbehavior activities such as dropping packets or delaying them. A node is said to be a malicious node, if a *threshold* number of neighboring nodes repot this node as having misbehaved activities.

In [9], the authors provide a protocol called mitigating colluding collision attacks (MCC) for wireless sensor networks. Where they improve the BLM techniques to mitigate the colluding collision attacks. In their proposed MCC protocol, the authors extend the number of guards from only the common neighbors of the relaying node and the next hop to include all the neighbors of the relaying node. Also the MCC protocol required each node to handle a counter for each neighbor, to be able to count the number of times that neighboring node is forwarding the packets that are not for its own use.

Most of the previous works have been proposed to work in wireless ad-hoc networks, such as wireless sensor network and wireless mesh networks, where the nodes are static with no movement. In this work, we realized that, *due to mobility, it would be hard for maintaining monitoring nodes such as guards or watchdog nodes, where in MANET all nodes are free to move in any direction, so it will be hard to keep watching nodes in the same neighborhood for along period of time*. Also we observe that, *maintaining a number of nodes in a neighborhood for a specific amount of time to watch the behavior of other nodes will restrict the nodes moving ability in MANET, which is unfair among the nodes in the network*.

III. Models and Motivations

First in this section, we will describe our network model and the adversary model. Then, formally we will discuss our motivations towards this work.

A. Network Model

We assume a large mobile ad-hoc network (MANET) that consists of a number of wireless nodes with moving ability (*each node is free to move in any direction*). Each node has the ability to store, process and relay packets to other nodes if it receives packets that are not for its own use.

We use an undirected bi-connected graph $G(V; E)$ to model the mobile ad-hoc network, where V is the set of n nodes and E is the set of m edges in the network. For each pair of nodes $(u; v)$, there exist an undirected edge $e \in E$ if and only if $d(u; v) \leq R$, where $d(u; v)$ is the euclidian distance between nodes u and v, and R is the transmission range of node $u(v)$. Each edge between any pair of nodes $(u; v)$ in G corresponds to a potential wireless link between nodes u and v in the network.

B. Adversary Model

To disturb MANET operations, the adversary may launch arbitrary attacks such as passive eavesdropping attacks [16] [20], or other active attacks which could be more harmful to the network, such as selective forwarding and black hole attacks [1] [4] [7]. In passive attacks, *due to the broadcast nature of wireless networks*, the adversary can capture any message within its range without being noticed by any other nodes in the network. On the other hand, the adversary can initiate an active attack that is more severe compared to the passive attacks [4]. In active attacks the adversary has the ability to capture/manipulate any message in its radio range, it also can inject new forged messages into the network [7].

In this work we focus on active attacks in MANET. We assume that, the adversary has the ability to compromise an arbitrary number of nodes, through physical capture or software bugs, thus gaining full control over them. Once compromised a node, the adversary will extract all the information stored in the compromised node as well as the encryption keys preloaded into its memory (*all its security information*).

In this work, we propose an active attack scheme named **C**olluding **I**njected **A**ttack (CIA) in MANET. The adversary will launch such an attack after finishing two consecutive

preparation phases, the *node replication phase* and the *node injection phase*.

After the adversary compromised an arbitrary node, it will access all its stored information. In the *node replication phase*, the adversary will inject a new replicated node, and store a copy of all the extracted security information from the compromised node into the memory of the new replicated node. The replicated node will not be active, until the adversary get rid of the original compromised node, by depleting its energy or isolating it, in order to make sure the replicated node will not be detected by any other node in the neighborhood. Following the first phase is the *node injection phase*, where the adversary will inject a new node (*not a replication of the compromised node*) into the network, which also has all the information stored in the compromised node.

These two malicious nodes will work together to launch a colluding attack on an arbitrary node in the network, to restrict its ability of receiving any packet, or relaying any packet. Our colluding injected attack (CIA) will be discussed in details in Section IV.

C. Motivations

In this section we discussed our motivations towards this work.

- In practice, upon compromising a node by an adversary, all the information stored in that node will be extracted, including the set of encryption keys preloaded to that node. We realized that, *upon extracting all the information from the compromised node, the adversary could generate a replicated node of the compromised node with a copy of all the extracted information from the compromised node*.
- A number of previously detection schemes have been proposed for detecting malicious behavior in static warless networks, in which nodes along the forwarding path (*nodes along the path from source to destination*) have to exchange multiple ACKs to detect the malicious node [22]. Mobility may affect such proposed detection schemes. *In MANET, each node is free to move and change in the neighborhood might occur, which makes it hard to maintain the same forwarding path that has been used before*.
- Previous studies in [9] [13], show that providing watchdog nodes in a network is a powerful technique in capturing misbehaving nodes. *Due to the mobility nature in MANET, it is hard to maintain watchdog nodes in a specific neighborhood, Since nodes are free to leave and change their neighborhood, Moreover, we observe that watchdog nodes fail to detect malicious behaviors in the presence of colluding attacks* [13]. The existence of colluding in a network will mislead the watchdog nodes if existed, where the colluding nodes will give an indication to the watchdog nodes that a legitimate node is misbehaving, *The colliding nodes will prevent an arbitrary node from receiving/relaying any packet, and since the watchdog nodes in this neighborhood will not hear any relaying packets from this node, they will report it as being malicious.*

IV. Colluding Injected Attack (CIA): How It Works

In this section we will show how our proposed colluding injected attack (CIA) works in MANET. CIA attack is launched after finishing two consecutive phases. First is, the *node replication phase*, in which the adversary will compromise an arbitrary node and then inject a replication node of the compromised node in the network. The second phase is the *node injection phase*, in which the adversary will inject another node that will work with the injected replicated node to restrict an arbitrary node's ability of receiving and relaying any packet. By doing this, *a legitimate node (the attacked node) might be reported as being malicious by any watchdog node if they existed in the neighborhood*, since they will not hear any forwards from the attacked node. Moreover, in reliable networks, (where the source node needs a conformation ACK packet from the destination to make sure that it receives the packet), if the attacked node is a destination node of an arbitrary communication, due to its inability of receiving any packet, *the source node might timeout before receiving any ACK from the destination node, thus may conclude that this destination node in unreachable*.

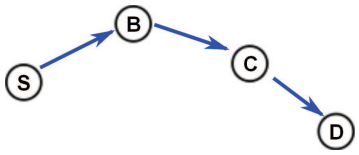

Fig. 2. Normal scenario

1) Node replication phase: The adversary has the ability to compromise an arbitrary number of nodes, through physical capture or software bugs, thus gaining full control over them. After compromising a node and accessing all its stored information, *the adversary will create a replication node of the compromised node and injects it in the network*. Note that, the adversary needs to isolate or deplete the energy of the compromised node, in order to make sure that his replicated node will not be discovered as a malicious node by any other nodes. Each replicated node injected by an adversary in the network will have more powerful prosperities compared to any other legitimate node in the network, such as the ability to communicate using different channels and sending using different transmission ranges.

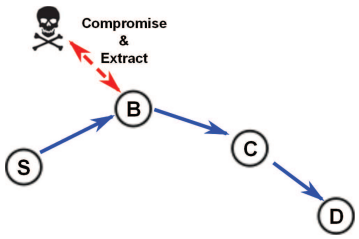

Fig. 3. The adversary compromised a node

We will use Fig. 2, Fig. 3 and Fig. 4 to illustrate the CIA's node replication phase. Fig. 2 shows the normal scenario, where node S is sending to node D through multihop using nodes B and C for relaying its packets. Normal legitimate sending is presented with blue solid arrows in the figures.

Let us assume that the adversary aims to attack node C. In order for the adversary to achieve his desired attack (*the CIA attack*) it will aim to compromise node B, which is the upstream node of node C on the path from the source node S and the destination node D. This can be seen in Fig. 3, where the adversary will compromise node B, and extract all its stored information, thus gaining full control over it.

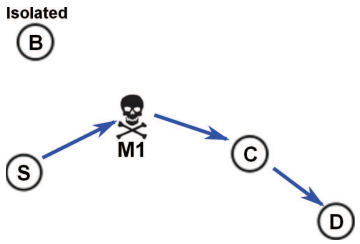

Fig. 4. The adversary injected a replicated node

After compromising node B and extracting all its information, the adversary will inject a replicated node (M_1) of the compromised node (B). To facilitate the communication of the replicate malicious node with other nodes in the network, the adversary will store a copy of all the information stored in node B into its new injected malicious node. This can be seen in Fig. 4. Note that, due to mobility and since the adversary has a full control over the compromised node (B), it will move the compromised node from its neighborhood and isolated it, and then brings its forged replicated node to the neighborhood to avoid being detected as a replica attack [21].

2) Node injection phase: The adversary will create another malicious node with a new identity that includes a copy of all the information extracted from the compromised node, and then it will inject this node in the network. Note that, this node is not a replication of the compromised node, but it has the same prosperities as the replicated node (*such as the ability to communicate using different channels and sending using different transmission ranges*).

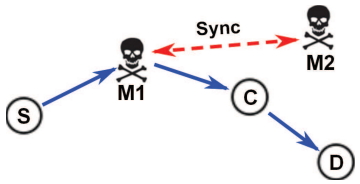

Fig. 5. Node injection phase

We will use Fig. 5 to illustrate the *node injection phase*. The adversary after injected the replicated node (M_1) in the network, it will create another malicious node (M_2) that has the same prosperities as the replicated injected node, and send it to the network. This new injected node (M_2) will work with the replicated injected node (M_1) to achieve the adversary's desired full CIA attack. To attack the network the adversary needs to synchronize the two injected malicious nodes to work together to achieve its desired attack. Note that, the synchronized message will be transmitted with a specific channel unknown to the other legitimate nodes. This is shown by the red dashed arrow in Fig. 5.

To achieve the full CIA attack, the adversary needs to maintain the following constrains to decide where to place its two colluding malicious nodes (M_1 and M_2), to make sure that they will not interfere with each other, but will create a collision at the attacked node.

- The euclidian distance between the malicious node (M_1) and the attacked node (C) should be less than or equal the malicious node's transmission range (R_1), which is given in Eq. (4.1).

$$d(M_1, C) \leq R_1 \tag{4.1}$$

- The adversary has to make sure that the transmission range of the second malicious node (M_2) is less than the normal transmission range (R_1). Which in turn is less that the transmission range of the synchronizing messages (R_{Sync}). This is given in Eq. (4.2).

$$R_2 < R_1 < R_{Sync} \tag{4.2}$$

- To make sure that the malicious nodes can send at the same time and will not interfere with each other, the adversary must satisfy Eq. (4.3). Where the second malicious node (M_2) should be out of the first malicious node (M_1)'s range.

$$d(M_1, M_2) \geq R_1 \tag{4.3}$$

Fig. 6 show the constraints needed injected malicious nodes placement decided by the adversary around the attacked node (C).

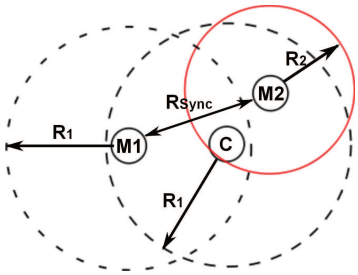

Fig. 6. Injected malicious nodes placement

The dashed circles in Fig. 6 show the transmission range (R_1) of nodes M_1 and C. Note that, here node M_1 will work normally as a legitimate node. The transmission of the malicious node (M_2) is given as R_2. The transmission range of the synchronizing messages between the malicious node is given as R_{Sync}.

Colluding Injected Attack (CIA): After finishing the preliminary phases, (the *node replication phase* and the *node injection phase*) the adversary will launch the main part of its CIA attack.

The CIA attack will affect the network in two different scenarios. To make it clear, we will use Fig. 7 and Fig. 8 to illustrate these two scenarios.

The *first scenario* is where the adversary attacks an intermediate node. This scenario can be seen in Fig. 7. Let us assume that node S needs to send some data to node D, but since

node D is out of the source node's range it must use other nodes to relay its packets. Node S will send the packets to the malicious node M_1 assuming it is the legitimate node B, at this time, the malicious nodes (M_1 and M_2) will exchange some synchronized messages, indicating *which node they are aiming to attack* and *when to start their attack*. Note that, after synchronizing the malicious nodes, the malicious node which received a packed to be relayed will work as a normal legitimate node, where on the other hand the other malicious node will launch the attack.

In our example in Fig. 7, let us assume that both malicious nodes agreed to attack node C. Node M_1 will work as a normal node, where it will relay the messages to node C, meanwhile node M_2 will start the attack. Before starting the attack, node M_2 will move closer to node C, to make sure that, by sending using a small transmission range only node C will receive its transmission. By the use of a small transmission range, the malicious node aims to hide itself from the watchdog nodes [14] or guard nodes [9] if they existed in the network.

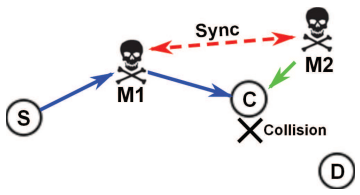

Fig. 7. CIA attack - First scenario

Both the malicious nodes will start sending to node C at the same time they agreed on when they exchange their synchronized messages, denoted with red dashed arrow in Fig. 7. Due to the wireless nature and the hidden node problem [3] [8] [12], a collision will occur at node C, where it will not be able to receive two messages from nodes M_1 and M_2 at the same time. Note that, since node M_2 is a malicious node, it will not follow any standard or exchanging any CTS/RTS packet before it sends any messages to node C. Node M_2's sending is denoted with green arrow in the figures.

Since node M_1 will relay the packets using the normal transmission range, all the neighboring nodes will hear that node M_1 is relaying the message. On the other hand, they will not hear any thing from node C (*node C is not relaying any packet*), since there was a collision at this node, and it was unable to receive any packet. And that results in having some doubts at the neighboring nodes that node C is dropping the packets and not delivering them, which may result in reporting the legitimate node C as being malicious.

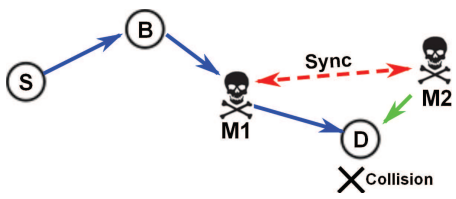

Fig. 8. CIA attack - Second scenario

The *second scenario* is where the adversary attacks a destination node. This scenario can be seen in Fig. 8. Let us assume that node S is sending using multihop to node D. The adversary has finished its two preliminary phases the *node replication phase* and the *node injection phase* and decided to attack node D. The two malicious node will create a collision at node D (the destination node), by sending at the same time, which prevents the destination node of receiving any packet designated to it. If the sender requested an acknowledgment (ACK) reply from the destination node for reliability purposes, it might timeout while waiting for a reply, since node D will not send any ACK back to the source because it was unable to receive any packet. In this case the source node can resend the packet again or simply will report that the destination node as unreachable.

V. Numerical Results

In this section, to illustrate the effect of our proposed **C**olluding **I**njected **A**ttack (CIA) on the network performance, we implemented our proposed attack in MANET, and show that this proposed attack cannot be detected by previous proposed malicious detection schemes [10] [13].

We considered a MANET with n nodes randomly distributed in a square playing field. Each node is free to move with a speed range: (1-5) m/s, and has a $250m$ transmission range. In our simulation, we implemented our proposed attack by injected two malicious nodes that collude together to attack a specific node. We set the number of packet to be sent on each connection to 100 packets. The results shown are average of 50 test runs. In our simulation, we allow the adversary to have the ability to attack the network multiple times in different time slots through the simulation time, in other words, *in one time the malicious nodes will work as legitimate nodes, and other time they will launch the attack*.

In this work, we defined the *false detection* of a scheme as the detection of a legitimate node as being malicious. To show how previously proposed detection scheme will perform against our proposed CIA attack, we used the *false prediction ratio* (FPR) as a performance metric, which is defined as, the ratio of the number of false detections of a scheme in the existence of an attack to the total number of attacks occurred in the network.

Our results are shown in Fig. 9. In these results, we implemented the watchdog scheme in [13] denoted as (Normal), in which a number of nodes are predetermined to work as a set of watchdogs nodes, where they will overhear the medium to check weather the next-hop node forwards the packets or not. We also implemented another detection scheme [10] denoted as (BLM 50%) in the figures. In the BLM scheme a set of nodes were assigned to work as watchdogs nodes, which are normal nodes in the network and perform their basic functionality in addition to monitoring. Malicious node's detection occurs after reporting by a threshold number of watchdog in the neighborhood. In our simulation we set the threshold to be 50% of the watchdog nodes in any neighborhood.

Our results in Fig. 9 show that, due to the occurrence of the **C**olluding **I**njected **A**ttack (CIA) in the network and the nodes mobility, increasing the number of watchdog nodes in

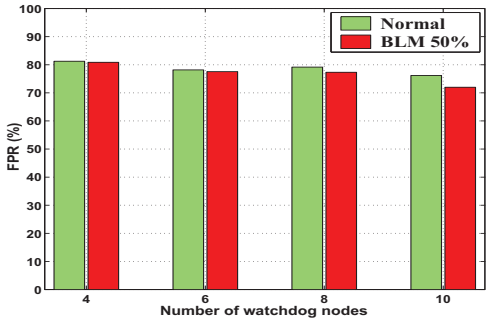

Fig. 9. False prediction ratio (FPR)

the neighborhood might help decreasing the *false prediction ratio*. For example, in BLM with the existence of 10 watchdog nodes in the neighborhood, the *false prediction ratio* has been improved by 7% compared to that with the existence of 8 watchdog nodes. Since all the nodes in the network are free to move and change their neighborhood, and to maintain the fairness of mobility among all the nodes in the network, any watchdog node may leave its neighborhood and move to another neighborhood, in other words is does not have much time to detect and report an existence of a malicious attack. Indeed due to the the CIA attack, and the existence of the colluding malicious nodes, which are creating a collision at an arbitrary node to prevent it from receiving any packet, this will mislead the monitoring watchdog nodes, and make them report a legitimate node as being malicious, since they might sense that the node is not relaying any packet which is not for its own use.

VI. Conclusion

In this paper, we proposed a Colluding Injected Attack (CIA), in which the adversary after compromising a legitimate node, it creates a replicated node and injected it into the network after isolated the compromised node, so no other node detects the existence of any node replication. Then the adversary will inject another node to collude with the replicated note to launch its attack, which aims to mislead previously detection schemes in reporting the attacked node which is a legitimate node as being malicious. Also by launching this attack around the destination node by the adversary, will prevent the destination node of receiving any packet from the source, thus will be unable to reply with any ACK message. In this situation, the source might conclude that the destination node is unreachable. Our simulation results showed that previously detecting schemes might be misled by our proposed colluding injected attack.

References

[1] G. Ács, L. Buttyán, I. Vajda, "Modelling adversaries and security objectives for routing protocols in wireless sensor networks," *SASN 2006*,pp.49-58.

[2] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, D. Barthel, "Secure Lossless Aggregation for Smart Grid M2M Networks," *SmartGridComm 2010*, pp.333-338.

[3] M. Cagalj, J. Hubaux, C. Enz, "Minimum-energy broadcast in all-wireless networks: NP-completeness and distribution issues," *ACM MobiCom 2002*, Atlanta, Georgia, USA.

[4] J. Cai, P. Yi, J. Chen, Z. Wang, N. Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network," *AINA 2010*, pp.775-780.

[5] L. Gao, E. Chang, S. Parvin, S. Han, T. Dillon, "A Secure Key Management Model for Wireless Mesh Networks," *IEEE AINA 2010*, Washington, DC. USA., pp.655-660.

[6] V. Gligor, "Handling new adversaries in secure Mobile ad-hoc networks," *ESNS 2007*.

[7] T. H. Hai, E. Huh, "Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge," *In Proceedings of the 2008 Seventh IEEE international Symposium on Network Computing and Applications 2008*, pp.325-331.

[8] L.J. Hwang, S.T. Sheu, Y.Y. Shih, Y.C. Cheng, "Grouping Strategy for Solving Hidden Node Problem in IEEE 802.15.4 LR-WPAN," *WICON 2005*, Washington, DC, USA, pp.26-32.

[9] I. Khalil, "MCC: Mitigating colluding collision attacks in wireless sensor networks," *IEEE GLOBECOM 2010*, December 2010, Miami, Florida, USA.

[10] I. Khalil, S. Bagchi, C. Nina-Rotaru, "DICAS: Detection, Diagnosis and Isolation of Control Attacks in Sensor Networks," *SecureComm 2005*, pp.89-100.

[11] D. Kim, H. Bae, J. Song, J. Cano, "Analysis of the Interaction between TCP Variants and Routing Protocols in MANETs," *In Proceedings of the 2005 international Conference on Parallel Processing Workshops*, June 2005.

[12] K. Kosek, "Problems with providing QoS in EDCA ad-hoc networks with hidden and exposed nodes," *INFOCOM 2009*, Piscataway, NJ, USA, pp.389-390.

[13] S. Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *MobiCom 2000*, New York, NY, USA, pp.255-265.

[14] A. Patcha, A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," *RAWCON 2003*, pp.75-78.

[15] T. Predojev, J. Alonso-Zarate, M. Dohler, "Energy-delay tradeoff analysis in embedded M2M networks with channel coding," *PIMRC 2010*,pp.2733-2738.

[16] H. Redwan, K. Kim, "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks," *In Proceedings of the 2008 Japan-China FCST08*, pp.3-9.

[17] A. Seddik-Ghaleb, Y. Ghamri-Doudane, S.-M. Senouci, "Effect of ad hoc routing protocols on TCP performance within MANETs," *SECON 2006*, vol.3, pp.866-873.

[18] M. Al-Shurman, S. Yoo, S. Park, "Black hole attack in mobile Ad Hoc networks," *In Proceedings of the 42nd Annual Southeast Regional Conference 2004*.

[19] Q. Wei, X. Wang, "The Design and Implementation of the Minimal M2M Terminal Based on the SIM4100 Wireless Module," *International Symposiums on Information Processing 2010*, pp.567-571.

[20] S. Xiao, W. Gong, D. Towsley, "Secure Wireless Communication with Dynamic Secrets," *INFOCOM 2010*, pp.1-9.

[21] K. Xing, X, Cheng, "From Time Domian to Space Domian: Detecting Replica Attaks in Mobile Ad Hoc Networks", *INFOCOM 2010*, pp.1-9.

[22] B. Yu, B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," *IPDPS 2006*.

[23] S.K. Zhang, J.W. Zhang, W. Li, "Design of M2M Platform Based on J2EE and SOA," *International Conference on E-Business and E-Government 2010*, pp.2029-2032.