American Journal of Applied Sciences 11 (8): 1391-1397, 2014
ISSN: 1546-9239

doi:10.3844/ajassp.2014.1391.1397 Published Online 11 (8) 2014 (http://www.thescipub.com/ajas.toc)

INTRUSION DETECTION IN MOBILE AD HOC NETWORK USING SECURE ROUTING FOR ATTACKER IDENTIFICATION PROTOCOL

[1]Gopalakrishnan, S. and [2]P. Ganeshkumar

[1]Department of ECE, PSNA College of Engineering and Technology, Dindigul, India
[2]Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, India

Received 2014-04-11; Revised 2014-04-26; Accepted 2014-05-29

ABSTRACT

In past few decades, the migration of communication takes place from wired networks to wireless networks because of its mobility and scalability and Mobile Ad hoc Network (MANET) is a unique and significant application in recent years which does not necessitates any pre-existing network infrastructure. Each node can act as both transmitters as well as receivers that are communicating with each other when they are in same communication/transmission range. Otherwise, these nodes depend on neighbor nodes to transmit their packets and they possess self-configuring ability which makes MANETs popular in various critical mission applications such as military and other emergency applications. In general, MANETs are open medium network and their nodes are widely distributed which makes the network more vulnerable to various attackers. Some times, the transmitted packets are viewed or modified or corrupted by the attackers through the way to reach destination and the destination could not find such type of packets. So, the receiver can deliver modified packets with wrong information. Thus, it is essential to present an efficient secure routing protocol to preserve MANET from several attacks. In this study, we are going to propose and implement a novel routing protocol named Secure Routing for Attacker Identification (SRAI) protocol that executes at receiver/destination side to discover the modified packets in delivered nodes and generate misbehaviour report to the source. Compared to modern approaches, SRAI protocol establishes higher attacker identification rates in certain considerations.

Keywords: MANETs, SRAI Protocol, Attacks, Security

1. INTRODUCTION

Generally, wireless networks possess flexible mobility and scalability for several communications. So, they are always chosen for various applications from the beginning of their innovation. These wireless networks are considered as an improved technology which has minimum cost for communication compared to wired networks and they gained more popularity in the field of research, industrial and academic. Mobile As hoc Network (MANET) is a significant concept of wireless networks which comprises of thousands of nodes that are mobile as well as autonomous and they do not requires any existing network infrastructure. The autonomous nodes can freely and randomly move within the network which can create temporary dynamic network and these networks can change their topology frequently (Miranda and Rodrigues, 2003). Each and every activity like node discovery and data delivery is performed by the autonomous nodes separately or conjointly.

The nodes of MANETs are fitted with both wireless transmitter as well as receiver which can communicate with each other through the wireless links in a direct or indirect manner and now-a-days industrial applications like remote access and control through the wireless links getting more fame. The MANET structure depends on their applications that may vary from modest, static network which is extremely power-consumed to large

Corresponding Author: Gopalakrishnan, S., Department of ECE, PSNA College of Engineering and Technology, Dindigul, India

scale dynamic mobile networks. MANETs are classified into two types such as open and closed in which the closed mobile networks are commonly used for emergency applications such as military and rescue services and their nodes get together towards a general destination. In an open mobile network, various mobile nodes work with several goals but they share common resources to assure worldwide connectivity (Kim, 2008; Jayakumar and Gopinath, 2007).

Moreover, the nodes of mobile networks can able to provide data communication among various users with constant mobility and after data communication it keeps their mobility as same level. This is the main advantage of wireless network over wired network. The communication is restricted to the nodes which are in various communication ranges and the mobile nodes can solve such problem by permitting intermediate nodes to execute data transmission (Ganeshkumar and Thyagarajah, 2010). This is done by splitting MANETs into two cases of networks such as single-hop and multi-hop. If the nodes are in the same communication range and can communicate directly with each other is considered as a single-hop network and in multi hop networks the nodes are in different communication range in which intermediate nodes are preferred for communication in an indirect manner (Sun, 2004).

Minimum constellation and frequent deployment create mobile network ready to be employed in emergency considerations where a substructure is not available or impracticable to establish in the following cases such as natural or human-caused tragedies, military battles and medical exigency conditions. Because of the above unique features, MANETs are widely employed in various industrial applications. However, believing the concept that MANET is famous within vital mission features, security of network is of much more important. Regrettably, the characteristics like open medium and remote dispersion of mobile networks causes it vulnerable to various attacks and the distributed architecture and frequently varying topologies, a conventional centralized monitoring approaches is no more executable in MANETs (Tabesh and Frechette, 2010; Kumar and Chockalingam, 2012). In this case, it is important to propose Secure Routing for Attacker Identification (SRAI) protocol which is particularly designed for mobile ad hoc networks.

Section 2, overview the operations of existing protocols. In section 3, vulnerabilities of MANET are discussed. Section 4 talk about the attacks in MANETs and section 5 reviews the algorithm of SRAI protocol. Section 6, shows the experimental results. Finally, section 7 concludes the paper and provides future works.

2. RELATED WORK

There are several works were conducted in MANETs to identify and solve the security related issues and some of them is presented here that are useful for constructing this study. Rai *et al*. (2010) presented a literature on attacks in MANETs and his work provides the elaborated definition of various attacks like behaviors of attacks and their consequences on mobile network features. He also explained a mechanism related to the security of MANETs for the attacks and the same topic is discussed in (Wu *et al*., 2006) and presented another literature of attacks in mobile networks. They also discussed about the attacks and security mechanisms. But they do not provide the simulation results and mathematical expressions. Konate and Abdourahime (2011) presented some simulation models of several attacks on mobile networks using NS-2 and are talked about the routing protocols and their resistances to various attacks rendered with analytical simulating and mathematical expressions.

Yuan *et al*. (2010) intrusion detection system which is based on Support Vector Machine (SVM) is proposed and the SVM is improved to attain higher security. Data is pre processed and similar data are removed in order to reduce the packet size (training data size) using k means clustering is proposed in (Muda *et al*., 2011) that demonstrate substantial advancement in training time to maintain accuracy. An important necessity of categorization is selection of parameters because some characteristics may be excess or with few efforts to the process of detection. Jemili *et al*. (2007) proposed Bayesian Network (BN) based intrusion detection scheme and such BN is employed to construct automatic intrusion detection system which is established on signature recognition system. The aim is to distinguish signatures of recognized attacks and it matches the signature with the detected signature. If it is similar then signal intrusion occurs.

3. VULNERA BILITIES OF MANETS

In wired networks, the communication takes place through wires and is flows through some other devices like gateways and fire walls. Thus, the security is maintained but we cannot employ wired networks for longer communication. So, we are going to the concept of wireless networks in which we particularly concentrate on Mobile Ad hoc Network (MANET) and because of the characteristics of mobile environment which are vulnerable that introduce several attacks like passive eavesdropping and active interfering Moreover, the nodes of MANETs can be attacked by various attackers from any directions. Some of the attacks like receiving access to secret information, message/content scrambling and activities of intermediate nodes like sender or receiver. From the above said we can clearly understand that mobile networks do not have an accurate line of protection. Hence, each and every node must be worked as supervisor/monitor. The mobile ad hoc network does not possess any pre-existing or centralized network architecture so their nodes can move through the network freely and randomly and can be attacked easily. It is somewhat difficult to maintain track of each mobile node in a world-wide network and the detection of particular attacked node. There is centralized node is present in such network so misbehaving node attack is possible as well.

4. ATTACKS IN MANETS

4.1. Tunneling Attack

Tunneling attack is also known as wormhole attacks which is nothing but when more than one node may cooperate to encapsulate and they interchange their messages among the nodes along existent paths. Such exploit provides the chance to a particular node or some nodes to make short-circuit and the actual flow of data constructing a virtual vertex cut in that network which is operated by the more than one colluding attacker nodes.

4.2. Information Disclosure Attack

In this information disclosure attack, an unauthorized node collects confidential data from compromised nodes in the mobile network. These data may contain the following information such as information concerning the network topology, nodes geographic location and best routes to unauthorized nodes in that mobile network.

4.3. Denial of Service (Dos) Attack

These attacks concentrate at the entire disruption of the function of routing and hence the complete operation of the mobile ad-hoc network. Particular examples of denial of service attack contain the overflow of routing table and the sleep privation torture. In overflow of routing table attack, the vicious node overflows the ad-hoc network with the creation of some bogus route packets to have the resources of the active node and interrupt the formation of decriminalize routes. The sleep privation torture concentrates at the batteries consumption of a particular node by invariantly maintaining it waged in routing conclusions.

5. PROPOSED PROTOCOL

In our paper, we proposed Secure Routing for Attacker Identification (SRAI) protocol that mechanically creates a misbehavior report to communicate the status of the obtained packets to corresponding source and such SRAI protocol conceives the threshold value of the transferred node that can be employed to discover the original packets at the destination side. For example, take a node that contains the threshold value as 30 and when it attains the receiver side, it assures the threshold value. If the checked threshold value is constant, then the destination takes over the delivered packet is original and creates an acknowledgement that is transmitted to that source. If these transmitted packets are watched or altered by any assailers by the way to reach their destination, its threshold value may vary and then it sent to the destination which assures the threshold value and discovers the obtained packet is replicate. Then, the destination makes a misbehavior report to corresponding source node.

5.1. Algorithm for Secure Routing for Attacker Identification (SRAI) Protocol

```
Collection of neighbor nodes $\Delta N_{ix}$
Initialize the source model $\Delta S_{ix}$
Attachment agent $\Delta R_{ax}$
Packet ID $\Delta P_{id}$
Nodes activity $\Delta N_{ix}$ in packet mode
$\Delta N_{ix} = \Delta P_{ckt}$
In packet mode
Total number of packets 1200
For ($\Delta P_{id} = 0; \Delta P_{id} < N; \Delta P_{id}++$)
Begin
If $P_{ckt} = A$
$P_{ckt} < =$ Attacker injected
send the misbehavior report and send the S-ACK //send duplicate report
Else
$P_{ckt} = B$;
$P_{ckt} =$ No attacker
Send (ACK) the acknowledgment packet ID
End if
End process
Destination $\Delta D_{ix}$
$\Delta D_{ix} < = \Delta R_{ax} + \Delta S_{ix}$
```

Generally, a mobile network comprises of thousands of mobile nodes in which any one of them acts as a source that can send packets through the network, a destination acts as a receiver and a router or an agent can acts as a forwarder of packets. When packet transmission takes place, the packets are transmitted from source to destination by the router or agent node and an acknowledgement is generated by the destination for corresponding node which is sent to the sender to know the status (like dropped or received) of the transmitted packets. While the source receives an acknowledgement for received packets then only it can send a next packet through the network to the destination. If suppose the transmitted packet is corrupted or hacked or modified by an attacker along the way to reach destination, such attacked packet is also transmitted to the receiver. In order to identify the attacked or modified packets at the receiver side we propose a protocol called Secure Routing for Attacker Identification (SRAI) protocol that automatically generates a misbehavior report to convey the status of the received packets to the source. This SRAI protocol considers the threshold value of the transmitted node which can be used to detect the correct packets at the receiver side. For instance, consider a node which has the threshold value as 50. When it reaches the destination, it checks the threshold value. If it is constant, then the receiver assumes the received packet is original and generates an acknowledgement which is sent to the source. If the packets are viewed or modified by an attacker through the way to reach destination, its threshold value may change and then it transmitted to the destination that checks the threshold value and identifies the received packet is duplicate. Then, it generates a misbehavior report to the source.

6. ISSUES IN TRADITIONAL METHODS

- It has lack of security while packet transmission
- By using such methods we cannot easily identifies the attacked packets as well as attackers
- The destination of the network can receive packets with some number of attacked ones
- The traditional methods do not generate any acknowledgement concerned with the status of received packets
- Throughput and efficiency of entire network is reduced

6.1. Benefits of Proposed Method

- Our proposed protocol provides more security while in transmission
- We can easily identify the attacked packets and attackers also
- The SRAI protocol can generate misbehavior report while it receives attacked packets
- Throughput and efficiency of entire network is increased when compared to the traditional methods

7. PERFORMANCE EVALUATION

The efficiency of the proposed protocol will be assessed using the performance evaluation by the following arguments: PDR, scalability, End-to-end delay and throughput.

7.1. Packet Delivery Ratio

It is specified as the ratio of data packets delivered by the receiver/destination which are provided by the sources and such performance measurement yields us an estimate of how well the protocol is executing in terms of delivery of packet at various speeds applying various traffic models.

7.2. End-to-End Delay

It is defined as the average time to reach data packet to the destination and lets in entire possible delays induced by buffering throughout the route discovery response time and queuing of the interface queue. Such metric is evaluated by deducting time at that first packet was transferred by the source of time at that initiative data packet came to destination.

7.3. Throughput

It is defined as the entire amount of packets obtained throughout the entire simulation time.

8. EXPERIMENTAL RESULTS

Figure 1 we compare the performance of networks that uses SRAI protocol and normal transmission and here we particularly compare packet delivery ratio and good put. The network that employs the SRAI protocol has high PDR and good put as compared with normal transmission.

Figure 2 we compare the performance of networks that uses SRAI protocol and normal transmission and here we particularly compare packet delivery ratio and scalability. The network that employs the SRAI protocol has high PDR and scalability as compared with normal transmission.

Figure 3 we compare the performance of networks that uses SRAI protocol and normal transmission and here we particularly compare end-to-end delay and packet sending rate. The network that employs the SRAI protocol has low end-to-end delay and packet sending rate as compared with the normal transmission.

Figure 4 we compare the performance of networks that uses SRAI protocol and normal transmission and here we particularly compare packet delivery rate and throughput. The network that employs the SRAI protocol has high PDR and throughput as compared with the normal transmission.

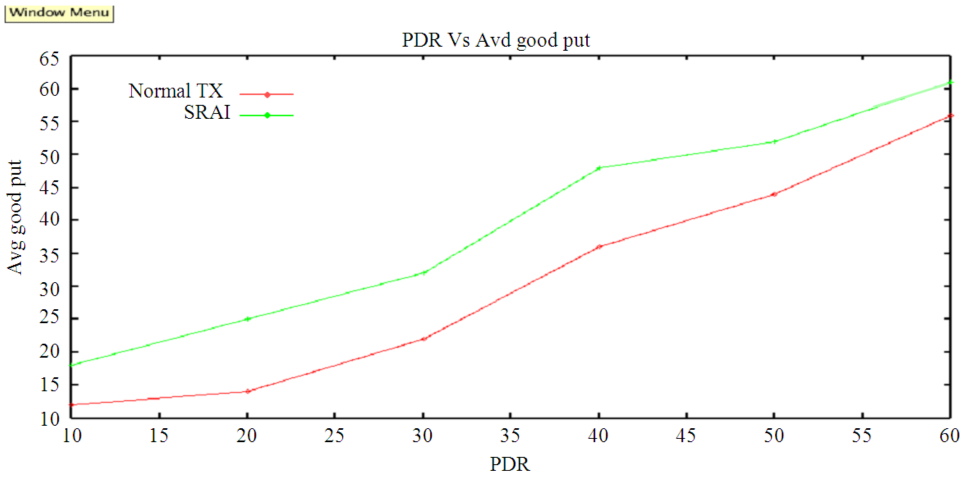

Fig. 1. Comparison between PDR and good put of Norma l transmission and SRAI protocol

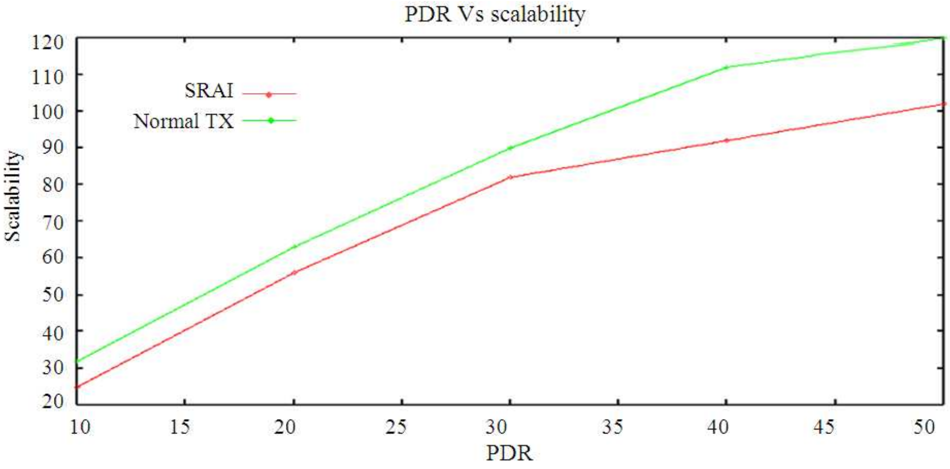

Fig. 2. Comparison between PDR and scalability of Norma l transmission and SRAI protocol

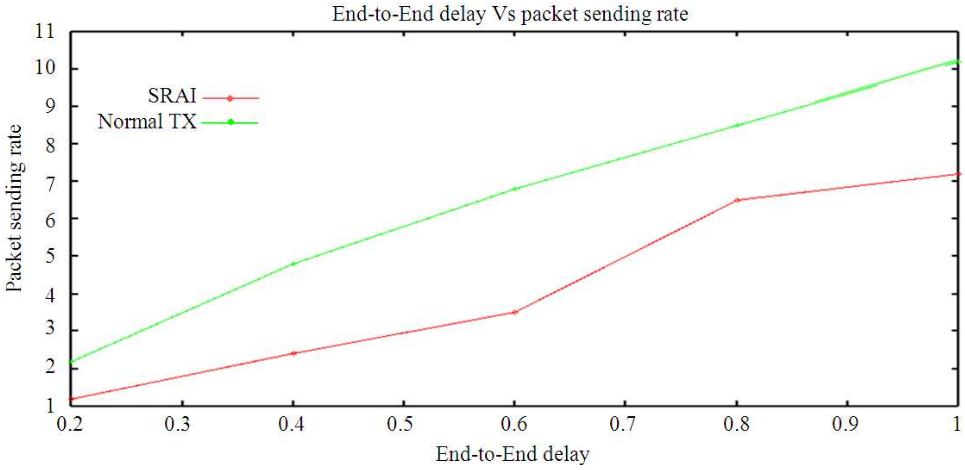

Fig. 3. Comparison between End-to-End delay and packet sending rate of Normal transmission and SRAI protocol

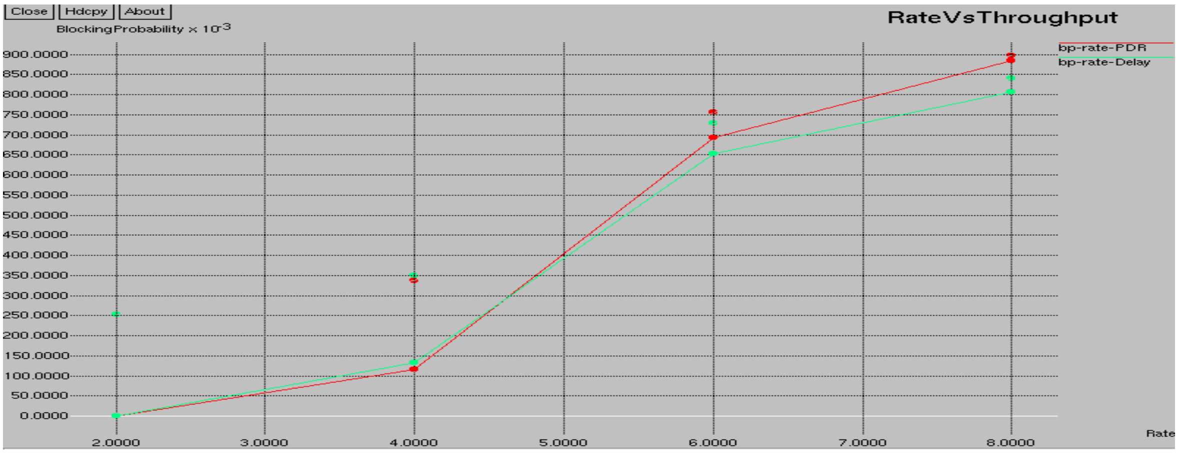

Fig. 4. Comparison between rate and throughput of norma l transmission and SRAI protocol

9. CONCLUSION

In MANETs, packet dropping or hacking causes a major threaten to the security and here we proposed Secure Routing for Attacker Identification (SRAI) protocol which is particularly designed for mobile ad hoc networks. By using the SRAI protocol, we can detect the attacked nodes at the receiver side by considering its threshold value and it automatically generates a misbehavior report to the source. When we compared this SRAI protocol to other existing attacker or intruder identification mechanisms, our proposed protocol provides better performance. In our proposed study, we only discover the modified or attecked nodes and generates misbehaviour report to acknowledge the source but in future, we extend our work to provide security in MANETs by proposing some authentication protocols.

10. REFERENCES

Ganeshkumar, P. and K. Thyagarajah, 2010. Balancing throughput and fairness for concurrent flows based on per flow scheduling in ad hoc networks. Int. J. Comput. Applic., 32: 408-415. DOI: 10.2316/Journal.202.2010.4.202-2856

Kumar, P.G. and S. Chockalingam, 2012. A collection of open research problems in rate based transport protocols for multihop ad hoc wireless network. Proceedings of the IEEE International Conference on Advances in Engineering, Science and Management, Mar. 30-31, IEEE Xplore Press, Nagapattinam, Tamil Nadu, pp: 125-131.

Jayakumar, G. and G. Gopinath, 2007. Ad hoc mobile wireless networks routing protocol-a review. J. Comput. Sci., 3: 574-582. DOI: 10.3844/jcssp.2007.574.582

Jemili, F., M. Zaghdoud and M.B. Ahmed, 2007. A framework for an adaptive intrusion detection system using bayesian network. Proceedings of the Intelligence and Security Informatics, May 23-24, IEEE Xplore Press, New Brunswick, NJ., pp: 66-70. DOI: 10.1109/ISI.2007.379535

Kim, Y., 2008. Remote sensing and control of an irrigation system using a distributed wireless sensor network. IEEE Trans. Instrum. Meas., 57: 1379-1387. DOI: 10.1109/TIM.2008.917198

Konate, K. and G. Abdourahime, 2011. Attacks Analysis in mobile ad hoc networks: Modeling and Simulation. Proceedings of the 2nd International Conference on Intelligent Systems, Modelling and Simulation, Jan. 25-27, IEEE Xplore Press, Kuala Lumpur, pp: 367-372. DOI: 10.1109/ISMS.2011.85

Muda, Z., W. Yassin, M.N. Sulaiman and N.I. Udzir, 2011. Intrusion detection based on k-means clustering and OneR classification. Proceedings of the 7th International Conference on Information Assurance and Security, Dec. 5-8, IEEE Xplore Press, Melaka, pp: 192-197. DOI: 10.1109/ISIAS.2011.6122818

Miranda, H. and L. Rodrigues, 2003. Friends and foes: Preventing selfishness in open mobile ad hoc networks. Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops, May 19-22, IEEE Xplore Press, pp: 440-445. DOI: 10.1109/ICDCSW.2003.1203592

Rai, A.K., R.R. and S.K. Upadhyay, 2010. Different types of attacks on integrated MANET-internet communication. Int. J. Comput. Sci. Security 4: 265-274.

Sun, B., 2004. Intrusion detection in mobile ad hoc networks. Ph.D. Thesis, Texas A and M Univ., College Station, TX.

Tabesh, A. and L.G. Frechette, 2010. A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator. IEEE Trans. Ind. Electron., 57: 840-849. DOI: 10.1109/TIE.2009.2037648

Wu, B., J. Chen, J. Wu and M. Cardei, 2006. A Survey of Attacks and Countermeasures in Mobile ad hoc Networks. In: Wireless Network Security, Yang Xiao, Xuemin Sherman Shen and Ding-Zhu Du (Eds.), Springer, New York, ISBN-10: 0387331123, pp: 103-135.

Yuan, J., H. Li, S. Ding and L. Cao, 2010. Intrusion detection model based on improved support vector machine. Proceedings of the 3rd International Symposium on Intelligent Information Technology and Security Informatics, Apr. 2-4, IEEE Xplore Press, Jinggangshan, pp: 465-469. DOI: 10.1109/IITSI.2010.72