ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Mitigating Malicious Activities by Providing New Acknowledgment Approach

G. S. Devi Lakshmi, J. Rajasekaran[2]

PG Student, Sri Subramanya College of Engineering and Technology, Palani, Tamilnadu, India[1]

Assistant Professor, Sri Subramanya College of Engineering and Technology, Palani, Tamilnadu, India[2]

ABSTRACT: New Ack scheme is efficient in finding malicious nodes and effective in transmitting the date in the presence of malicious nodes. In MANET data transmission in the presence of malicious nodes is the major problem. In existing watchdog scheme, there are two parts namely watchdog and pathrater. The watchdog detects the malicious node. If it next node is fails transmit the data means it increase the failure counter and also if a particular fails to transmit the data within a particular period of time means also it increase the failure counter and marks that node as an malicious. Pathrater task is just filtering the malicious node from the future transmission. If pathrater filtering the malicious node and transmission will be with the low transmission power and collision occurrence is more. N the proposed Enhancement two schemes are used first scheme identifies the malicious node and generates malicious report. Second scheme verifies the malicious report and authenticates the sender that the particular node is malicious and finds a path to transmit the data in MANET.

KEYWORDS: MANET, malicious node, pathrater, watchdog, malicious report

I.INTRODUCTION

The improved technology and reduced costs, wireless networks have gained much more preferences over wired networks in the past few decades. By definition, Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations. Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs**.**

The remainder of this paper is organized as follows. Section II reviews Watch dog scheme [19]. After that, we present two new schemes in Section III. Then, the details of improved scheme are given in Section IV. Finally the conclusion is given in Section V.

II.WATCH DOG SCHEME

Watchdog aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

III. PROPOSED IMPROVEMENT

IDEA:

In previous existing watchdog scheme it just increases the failure counter. It waits for the next node for its transmission if it fails to transmit within a certain threshold value it increases the failure counter. Our proposed IDS transmit data in the presence of malicious node. There are two schemes mainly available,

1. S-Ack
2. MRA

These two schemes used to find malicious node and used to re-transmit the data. Whenever a malicious node is identified in the network S-Ack will be generated. For every S-Ack an MRA report will be generated. From this report we can identify that particular node is malicious.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

ARCHITECTURE DIAGRAM:

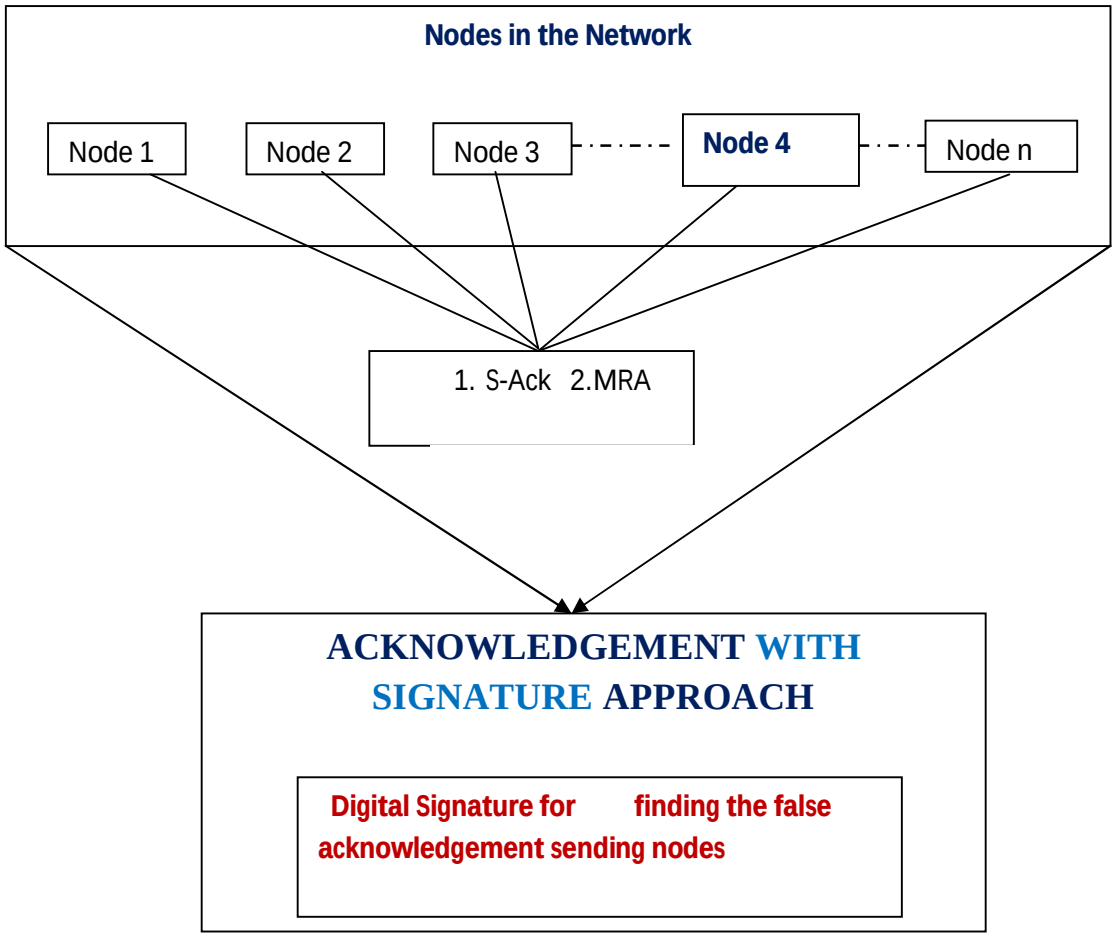

Fig 1-Architecture of proposed system

IV. DETAILS OF THE PROPOSED SYSTEM

In our framework, We define some terms for the senders and receivers for efficient transmission.

1. Node Initialization:

Mobile computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

communication sessions with servers which await (listen to) incoming requests. The followings are the parameters to construct a network.

- Node Name
- Host Number
- IP Address

All the communicating nodes re initialized by the properties of node name, host number and IP address.

2. Message Transaction:

Message Transaction is nothing but sending and receiving messages between nodes. This transaction will be run successfully by sending acknowledgement reports of all the nodes.

3. Attacker Module:

A person that is interested in attacking your network; his motivation can range from gathering or stealing information, creating a DoS, or just for the challenge of it. Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur. In this module the attacker node is deployed to show the acknowledgement based attacks.

4. Acknowledgement Verification:

There are several forms of acknowledgement which can be used alone or together in networking protocols:

- Positive Acknowledgement: the receiver explicitly notifies the sender which packets, messages, or segments were received correctly. Positive Acknowledgement therefore also implicitly informs the sender which packets were not received and provides detail on packets which need to be retransmitted. Positive Acknowledgment with Re-Transmission is a method used by TCP to verify receipt of transmitted data. PAR operates by re-transmitting data at an established period of time until the receiving host acknowledges reception of the data.

- Negative Acknowledgment (NACK): the receiver explicitly notifies the sender which packets, messages, or segments were received incorrectly and thus may need to be retransmitted.

- Selective Acknowledgment (SACK): the receiver explicitly lists which packets, messages, or segments in a stream are acknowledged (either negatively or positively). Positive selective acknowledgment is an option in TCP that is useful in Satellite Internet access.

- Cumulative Acknowledgment: the receiver acknowledges that it correctly received a packet, message, or segment in a stream which implicitly informs the sender that the previous packets were received correctly. TCP uses cumulative acknowledgment with its TCP sliding window.

- But EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- These acknowledgements are used to verify the packets which are sending to the destination whether those packets are sent successfully or not sent or else they are lost in the network. So, in order to verify the packets and to resend the packets we are using these types off acknowledgement verification scheme.

5. False report Authentication by the proposed protocol:

The proposed protocol will generate the digital signature by its own verify the digital signatures by itself. So that each node need not to share the digital signature keys to other nodes because protocol itself verifying the nodes automatically.

V. CONCLUSION

In this paper we proposed two Ack schemes for improving the watchdog scheme. The first scheme identifies the malicious node and will generate a misbehavior report. The second scheme verifies the misbehavior report and reports the sender that the particular node is misbehaving. And also finds another path form source to destination for the transmission. Thus these two schemes improve the transmission in MANETs in the presence of malicious nodes.

REFERENCES

[1] Al.Agha, M.H.Bertin, T. Dang, A. Guitton, P.Minet, T.Val, and J.-B.Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[2] R.Akbani, T.Korkmaz, and G.V.S.Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127.New York: Springer-Verlag, 2012, pp. 659–666.

[3] R.H.Akbani, S. Patel, and D.C.Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana,India, 2012, pp. 535–541.

[4] T.Anantvalee and J.Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: Springer-Verlag, 2008.

[5] V.C.Gungor and G.P.Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," *IEEE Trans. Ind.Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[6] Y.Hu, A.Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2002, pp. 12–23.

[7] G. Jayakumar and G. Gopinath, "*Ad hoc* mobile wireless networks routing protocol—A Review,"*J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582,2007.

[8] S. Marti, T.J. Giuli, K.Lai, and M.Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.