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

A Survey on Intrusion Detection in Mobile Ad Hoc Networks Using Enhanced Adaptive Acknowledgment

B. Sindhu[1]

M.E, Karpagam University, Coimbatore, India[1]

ABSTRACT: In modern technology, wireless network used for effective communication. MANET [Mobile Ad hoc Network] plays a vital role in wireless communication. From mobile ad hoc network can used to fix a random node with mobility condition. All the nodes should occur in mobility and scalability. Any node can move from one place to another place without any link failure. At the same time any code can act as a misbehaving node due to malicious attackers. This is the major drawback in Mobile ad hoc network. To overcome these issues introduced a new scheme as authenticate secure acknowledgement ASA algorithm. From these algorithm can able to find out the malicious attackers correctly from the source to destination. Also analyze the performance of the entire network using simulation parameters such as packet delivery ratio and routing overhead.

KEYWORDS: Authentication, Secure Acknowledgment, Malicious Node, Attacker Detection, routing overhead.

I. INTRODUCTION

An ad-hoc network is a collection of wireless mobile nodes dynamically forming a temporary network. In this network topology may change rapidly due to mobility condition. Here all the nodes act as either source or destination; it will transmit and also receive the packets simultaneously. It does not have any centralized infrastructure and used to generate distributed network. In centralized, nodes will transmit the packet via center server and also dependent. But in MANET used to transmit the packets from source to destination via intermediate nodes and also independently. It will randomly create the topology based on the routing table source will transmit the packets to the destination.

Figure 1 shows the [MANET] Mobile Ad hoc Network architecture. S denotes the source, D denotes the destination between the source and destination nodes are intermediate nodes act as co-operative nodes. All the mobile nodes are generated randomly in a dynamic architecture. An intermediate node does not transmit the packet in a certain time, intruders may attack the node and the packet will be lost.

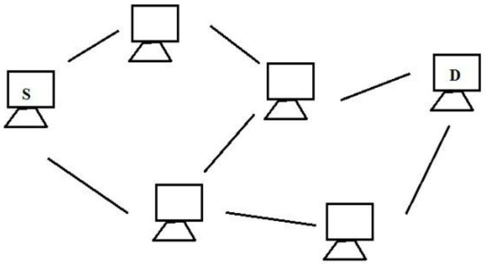


Figure 1: MANET

Security in a MANET is an essential component for basic network functions like packet forwarding and routing: network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. Other networks using dedicated nodes to support basic functions like packet forwarding, outing and network management in ad hoc networks those functions are carried out by all available nodes.

II. RELATED WORK

R. Akbani et.al, [1] discuss about security issues in the mobile ad hoc network. The nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. This algorithm discusses the security criteria of the mobile ad hoc network and presents the main attack types that exist in it. Finally this algorithm suggests the current security solutions for the mobile ad hoc network. S. Patel, et.al, [2] describes clearly security is the major issue in mobile ad hoc network due to the lack of centralized infrastructure. Mobile ad hoc network consists of distributed architecture. Any node can enter/leave the network and also all the nodes can act as either intermediate or cooperative nodes. To get a secure transmission this algorithm suggests the types of attacks. From these types can able to rectify the malicious node. T. Anantvalee et.al, [3] suggest the use of mobile ad hoc networks (MANETs) has mostly used in military application. In military appliances requires more security than other application. Due to that security introduced the new scheme which is mainly focused on the malicious node detection.

V. C. Gungor et.al, [4] explains about the today's competitive world facing demands of individual company related to low cost and high efficiency. So he proposed a new technique is industrial wireless sensor networks technology. Due to this can easily adapt in any environment. Compared to wired, it is more efficient in self organization, flexibility and rapid deployment. And these techniques were applied in hardware method also. It is user friendly. Owner can adapt easily using this method. Without the owner permission no one can access this technology. So security is more concern in this technique.

D. Johnson et.al, [5] discuss an ad hoc network consist of mobile nodes without any infrastructure. It does not focus on centralized infrastructure. In centralized all the nodes should get permission from centralized node to transmit the packets. But in distributed any node can move anywhere within that coverage area without asking anyone. Due to this security is major drawback in the mobile ad hoc network. This algorithm [8] presents a protocol to make a routing table using dynamic source routing. It is very frequent and also it contains hop count, distance, alternate path and traffic between the source and destination. Here simulate this concept using ns2. From that simulation results analyzed the host performance of that network. It's having low overhead during the time of low mobility. When it starts to increase the high rates of mobility packets transmitted rate was decreased.

III. EXISTING SYSTEM

To increase the throughput and to detect the malicious node used traditional scheme was watchdog [7]. In MANET source will transmit the packets through intermediate nodes to the destination. Using Watch dog technique after forwarded to the intermediate node it will receive the acknowledgment from the intermediate node.

Then only it allows the next transmission. If the intermediate node does not send the acknowledgement within a certain time it will decide that particular intermediate node as malicious node. Suppose due to overhearing it may take certain time to send an acknowledgment, watch dog technique wrongly decides the particular intermediate node as malicious node. To overcome these issues generate a new technique defined authenticate security acknowledgment.

3.1 Issues

The major drawbacks of watch dog technique are limited transmission power, false misbehavior report, Collusion and Partial dropping.

3.2 Motivation

For secure transmission should detect the malicious nodes and also remove that node to transmit the packets without any interruption. Malicious node normally generates to make the packet lost between the source and destination.

To avoid this type of lost focusing on security authentication.

IV. PROPOSED SYSTEM

The proposed technique is used to overcome the major drawbacks of watchdog technique. Figure 2 shows the proposed scheme used to receive after the acknowledgment only it will transmit. Within a particular threshold it does not receive the acknowledgment proposed scheme introduce the second step to decrease the transmission power. Source will send the secure packet to next three intermediate nodes. After a certain time if it will receive the secure acknowledgment

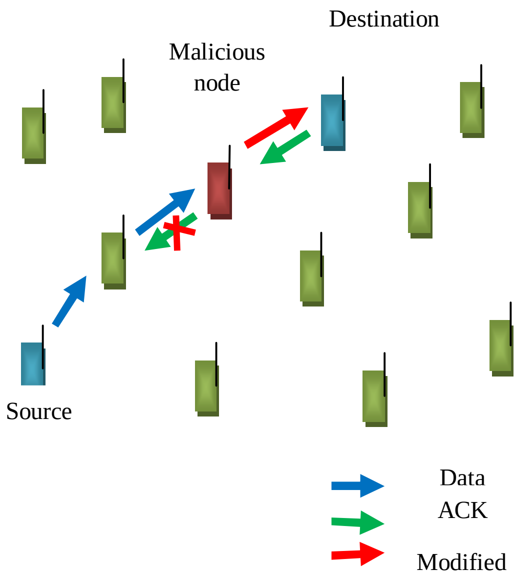


Figure 2: System Architecture

there is no misbehavior node between the source and destination. If suppose source node does not receive the secure acknowledgment that will report the intermediate node as malicious node. To avoid the false misbehaving report using DSR routing protocol find new path from source to destination. From new path it will forward the same packet to the destination after that it will whether these packets already received or not in the destination. If these packets already received misbehaving report was false otherwise misbehaving report was true. So from that new proposed algorithm can able to check the misbehaving report condition also. In this proposed technique divided into three steps. Step 1: waiting for an acknowledgement with a particular threshold. Step 2: source will generate a secure acknowledgment scheme and Step 3: using DSR protocol check whether the misbehaving report was false or true.

4.1 Node Generation and Configuration

The number of nodes can be generated using node creation command in ns2. For MANET, wireless and mobile nodes has to give some configuration like routing protocol, MAC layer type and omni directional antenna.

4.2 AS (Acknowledgment Scheme)

AS is used to check whether the packets successfully delivered or not. In AS method, node S sends a data packet Pak to the destination node D. all the nodes between the source node and destination node is co-operative node which is used to route along the packets. D successfully receives Pak, node D is required to send back an ACK acknowledgment packet Ack along the same route but in a reverse order. Within a particular time period, if node S receives Ack, then the packet transmission from node S to node D is successful. Otherwise, source node will switch to G-ACK mode by sending out an G-ACK data packet to detect the misbehaving nodes in the route.

4.3 G-ACK (Group-Acknowledgment)

The G-ACK scheme is mainly focused on to detect the misbehaving nodes in a network. Group of three nodes used to find out the misbehaving nodes so it is called as G-ACK scheme. It selects three consecutive nodes from that third node it should get the secure acknowledgment. Figure 3 shows for every three consecutive nodes in the route, the third node is required to send a secure acknowledgment packet to the source node. To reduce the receiver collision and transmission power introducing the G-ACK scheme.

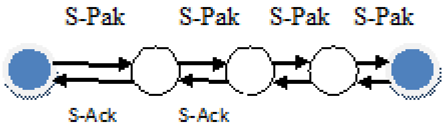


Figure 3: G-ACK

4.4 MND [Malicious Node Detection]

The MND scheme is designed to overcome the drawbacks of Watchdog when it fails to detect misbehaving nodes with the presence of false malicious node.

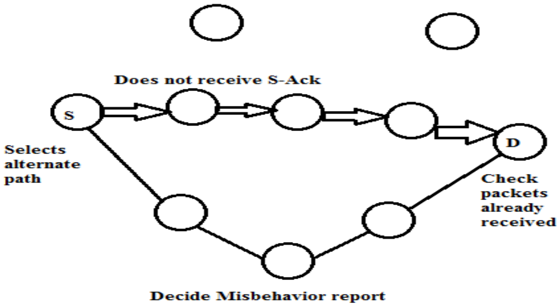
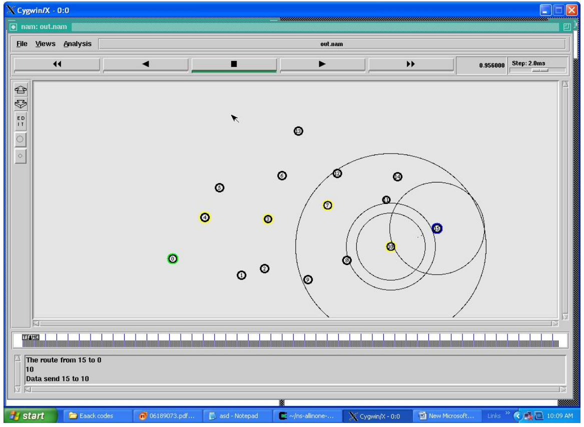


Figure 4: MND scheme

Figure 4 shows the scheme of MND concept is used to find out whether the misbehaving report is correct or not. After the G-ACK scheme within a particular threshold time it doesn't receive a secure acknowledgment it will decide the some malicious node can affect the path and also it gives the report as misbehaving nodes in that network. Using this MND scheme, analyze the G-ACK report. To initiate the MND mode, the source node using DSR routing protocol find an alternate path to reach the packets. DSR protocol used to generate the routing table with the possibilities of routing path between the source and destination. MND scheme starts to search an alternate path from a routing table of DSR routing protocol. After selecting an alternate path it starts to transmit the packets to the destination node. After the packets received successfully in the destination node, it starts to check these information packets already receive or not. If it received the packets already G-ACK report was incorrect. If suppose, packets are not received earlier in that destination node. G-ACK misbehavior report was accept and trusted.

V. EXPERIMENTAL RESULTS

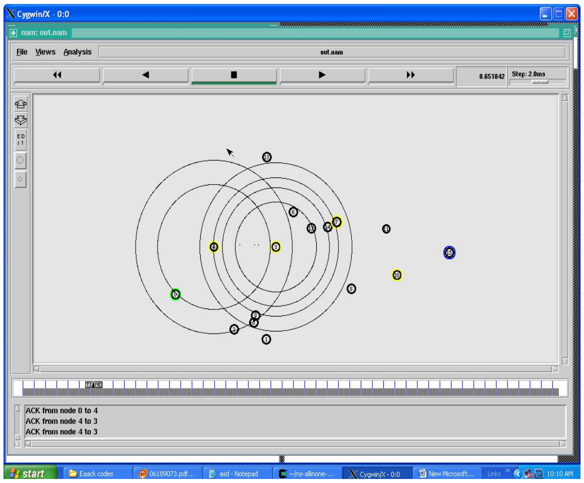
During simulation time the events are traced by using the trace files. The performance of the network is evaluated by executing the trace files. The events are recorded into trace files while executing record procedure. In this procedure, we trace the events like packet received, Packets lost, Last packet received time etc. These trace values are write into the trace files. This procedure is recursively called for every 0.05 ms. so, trace values recorded for every 0.05 ms.



The route from 15 to 0
10
Data send 15 to 10

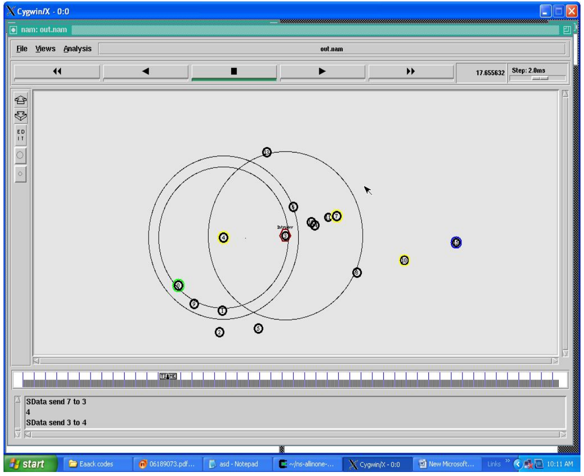
Figure 5: Proper route

Figure 5 shows the screenshot of proper route from source to destination. Here node o is the source node 15 is destination from source to destination it will select the proper route and start to transmit the packets via intermediate nodes Figure 6 shows the acknowledgement scheme. After packets received the destination it will send the acknowledgment to the destination. If the source doesn't receive the acknowledgment source will decide may intruder attacks the intermediate node.



```
ACK from node 0 to 4
ACK from node 4 to 3
ACK from node 4 to 3
```

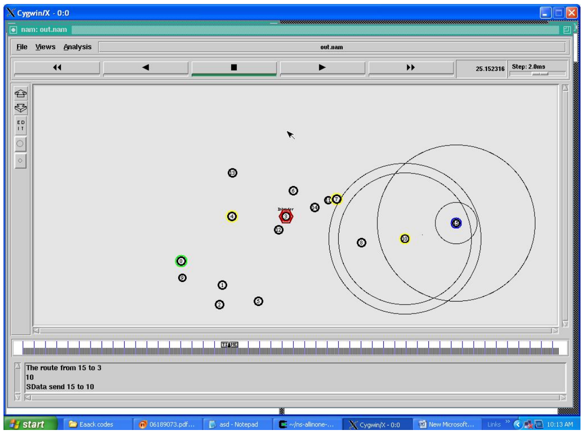
Figure 6: ACK scheme



```
SData send 7 to 3
4
SData send 3 to 4
```

Figure 7: Malicious node Detected

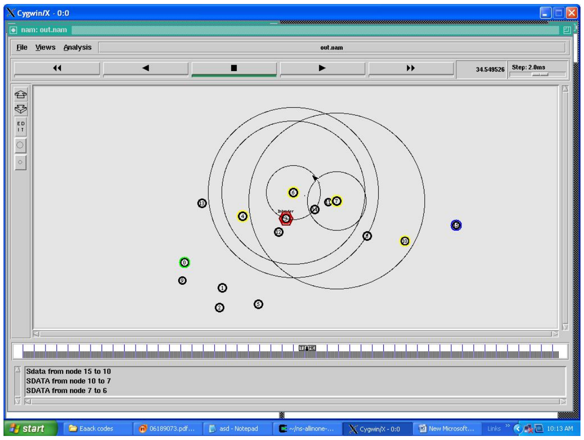
Figure 7 show that malicious node detected. If source node does not receive the acknowledgement after a certain threshold, it detects the malicious node occur between the source and destination.



```
The route from 15 to 3
10
SData send 15 to 10
```

Figure 8: G-ACK scheme

Figure 8 shows the G-ACK scheme. Here source node starts the security packet to the three consecutive nodes between the source and destination. Again the source node will wait for a particular threshold it does not receive the G-ACK and decide the node as misbehavior node.



```
Sdata from node 15 to 10
SDATA from node 10 to 7
SDATA from node 7 to 6
```

Figure 9 MND scheme

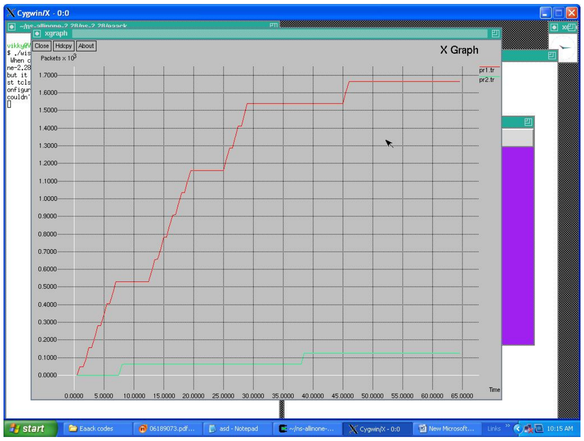


Figure 10: Packets transferred

Figure 9 shows the malicious node detection [MND] scheme. In this scheme using DSR protocol it will select another route for transmission. In the destination node it will check these packets are already received or not. In this destination node does not receive the packet already because of malicious node. Source decided that misbehavior report was correct.

Figure 10 shows the comparison graph between number of packets received in proper transmission and after the malicious node detection.

VI. CONCLUSION

In MANET security is the major issue. Due to this malicious node major drawback is packet dropping in mobile ad hoc network. To overcome this proposed new algorithm is authenticate secure acknowledgment ASA algorithm contain three steps expecting acknowledgment after that secure acknowledgment. Then authenticate the report generate a alternate path decides a misbehavior report correctly. The results were simulated shows the positive performance against previous technologies like watchdog technique and two ACK techniques which is used to overcome the receiver collision, low transmission power and false misbehavior report. Furthermore, using this MND scheme to easily detect the misbehavior report was true or false. Simulation results show that correctly decides the misbehavior report. Packets drop rate and packet transferred rate was analyzed using ns2. Here also using digital signature scheme for secure transmission. From this algorithm can decide the correct malicious node between the source and destination. In future recover that malicious node and make a proper transmission between the source and destination to overcome the packet drop rate, transmission power and overheads.

REFERENCES

[1] 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.

[2] 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.

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

[4] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[5] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[6] 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.

[7] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.

[8] 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.

[9] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.

[10] M. Zapata and N. Asokan, "Securing *ad hoc* routing protocols," in *Proc.ACM Workshop Wireless Secur.*, 2002, pp. 1–10.