A NOVEL APPROACH FOR A SECURED INTRUSION DETECTION SYSTEM IN MANET

Renjini Rajendran[1], Ragesh G.K[2]

[1]*Student, Computer Science and Engineering, Adi Sankara Institute of Engineering and Technology (ASIET) Kerala*
[2]*Asst. professor, Electronics and Communication Engineering Department, Adi Sankara Institute of Engineering and Technology (ASIET) Kerala, India*

Abstract

Mobile Adhoc Network (MANET) is a collection of wireless mobile computers (nodes) in which each node communicate with the other nodes in the network through radio waves. Here each node in the network is independent and thus it does not rely on each other for moving across the network. The most important attractions of MANETs is that they can be deployed with less effort as these network have no fixed infrastructure and are decentralized in their functioning. Each node in the network are capable of acting as both a sender and also as a receiver. The characteristics of MANETs such as: Scalability, dynamic topology, node mobility, and self-organizing capability of MANET made it widely accepted among applications like military environment, disaster relief or emergency recovery. The set of applications for MANETs can range from small-scale, static networks to large-scale, highly mobile networks. But the easily accessible peer to peer network and the large scope distribution of mobile nodes made it vulnerable to both external and internal attacks. In this paper, an efficient intrusion detection system (IDS) was being proposed and implemented which promotes complete unlinkability and is also capable to conceal the contents of all types of packets transmitted across the network. Thus it adds a private preserving feature to the IDS which enables the packet to be transmitted in the network with all the privacy and security required. The proposed scheme uses a novel combination of group ID and digital signature-based encryption for route discovery. This scheme enables the malicious node to be detected during the route discovery phase and avoids these nodes during the data transmission. Thus the proposed scheme promotes a secure transmission through the network. Compared to existing approaches the proposed scheme demonstrates a very low end to end delay and also significantly improves the packet delivery ratio.

Keywords: *MANET, Intrusion Detection System (IDS), unobservability, Group signature, encryption*

----------***----------

1. INTRODUCTION

Wireless communication networks have become popular and are also expected to gain more popularity in the future. This is due to its primary feature of rapid generation and destruction capability. Thus MANETS can be generated at a very fast rate and can also be destroyed easily after its use. Thus the dependence on MANET has been increased drastically. The applications for MANET include in business environment for a collaborative task, crisis management which include emergency, disaster or in military application. MANETs are also used in PAN(personal area networking). Such network does not depend in centralized or organized functioning.

A MANET is an independent and intelligent collection of mobile nodes which communicate with each other through radio waves via bidirectional links. As the nodes are mobile there is no fixed topology for these networks. The shape and size of the network keeps on varying with time. Similarly the decentralized characteristics of the network imparts the routing functionality such as route discovery is imparted on every nodes. And thus each node is responsible for its own transmission. There is no central node to take care of the detection and avoidance of the malicious node. MANET's are temporary networks with self-organizing and self reconfiguring capability. The highly dynamic characteristics of nodes in these networks makes it difficult to design a suitable network protocol for such networks. MANET's usually span across a fixed communication range. Each node must also be able to access and communicate with all the nodes within this communication range. This necessity adds more complexity since position of the nodes are not fixed and thus the connectivity pattern also becomes dynamic. MANETs require efficient distributed algorithms to determine network organization, link scheduling, and routing. Usually in static networks optimal route from source to destination was determined by finding the shortest route between them. But this concept is not applicable for MANET's.

Issues such as changing and fading wireless link quality and topology, propagation path loss, multiuser interference, power constraints are the other critical factors which makes the design of routing problems more complex. MANETS relies on wireless transmission for message transmission. Hence the transmission of packet across the network must be made secured so that the contents of the packet are not revealed to an external node. This helps in preserving the privacy of the nodes.

The attacks in MANET can be classified into two types namely passive attacks and active attacks. Passive attacks are attacks which does not alter the contents in data packets.

Some Examples of passive attacks include traffic analysis and eavesdropping attacks. Such attacks listen/monitor the conversation between source and destination nodes. Active attacks are those attacks which alter the data packets being sent by the source. As a result the data packets may be manipulated before it reaches the destination Some examples of active attacks include selfish node attacks, black-hole attack, forged acknowledgment attacks. Selfish node attacks the attacking nodes uses its resources for the its own transmission of packets. The selfish node may accept the packet from another node and ignores its transmission. Hence selfish nodes does not forward the packets if that particular transmission is of no use to the attacking nodes. In forged acknowledgment attack an intermediate node may manipulate the original acknowledgment packet send by the destination and forges a new acknowledgment. This acknowledgment packets are forwarded to the sender. The sender may fail to determine that the acknowledgment received was not the original acknowledgment being send by the destination node. Blackhole (packet dropping)attack is one of the types of packet drooping attack. Here the router drops all the packet that it receives instead of forwarding it.

The identities or intensions of the Mobile devices cannot be predetermined or verified. The cooperation among the nodes in the network is a main concern to maintain the But there are certain nodes which refuses to cooperate by not forwarding packets to the other nodes and thus it preserves its resources from getting exhausted. The other factors that increased the complexity of a secure data transmission across the wireless networks include the dynamic nature of the nodes, limited power, and limited availability of resources. Thus integrity can be preserved only if the nodes cooperate with each other.

2. EXISTING SYSTEM

In [3], Lidong Zhou and Zygmunt J. has discussed the attacks, threats in an ad hoc network. It also specifies the goals which to be attained to maintain the security in the network..The challenges, shortcomings and opportunities of this new networking environment are identified and explored to design a new approache to secure its communication. Also it takes advantage of the inherent repeatation in ad-hoc networks and multi-route existence between any pair of nodes in the network to prevent routing against denial-of-service attacks. This redundancy and multiroute existence can also be used to tolerate against the Byzantine failure..A secure and easily available key exchange schemes are developed by including replication and new cryptographic schemes, such as threshold cryptography. But the focus is mainly on two issues, ie how to secure routing and on how to establish a secure key management scheme in an ad hoc networking environment. Security goals can be achieved only by satisfying these two issues. More work are to be done to include these security schemes in an ad hoc networking environment and to investigate the impact of these scheme and performance of the network on its inclusion.

Generally each nodes in the MANET assumes that all other nodes cooperate in forwarding data and hence considers them trustworthy. This provides attackers with the opportunity to attack the network by just compromising two or three nodes within the MANET. Thus the attack will be generated internally within the MANET. To overcome this problem an highly efficient IDS must be included within the MANET's thus enhancing the security. If MANET are made capable to detect the attackers as soon as they enter the network, then it is possible to completely eliminate the cost of destruction generated by the compromised nodes to the network. IDSs are considered as the second layer in MANETs, and hence this benefits the existing proactive approaches. A number of intrusion detection schemes were developed for secure routing. Many of the intrusion detection scheme depends on acknowledgment send by the destination to the source node. The normal end to end acknowledgment scheme(ACK) sends a packet from source to destination. Once the packet reaches the destination, the destination node are required to send back acknowledgment to the source node in the reverse direction of the same route through which it reached the destination node. But if the acknowledgment is not received by the source within a pre-defined period then it is possible to conclude that some misbehaving activity occurs in the network. But this scheme was not able to detect intrusions in the precense of forged acknowledgment and false misbehavior report. Also this scheme generates a high network overhead.

A number of intrusion detection schemes are based on acknowledgments such as TWOACK, 2ACK, SACK , EAACK etc.

1. WATCHDOG [8]: It was designed to detect and avoid the malicious(misbehaving) nodes in the network. This detection was done by listening to the next hop's data transmission. If the node was found not transmitting the packet that was sent then a counter value was incremented. When the counter value exceeds a certain threshold value the misbehaving node will be excluded in the future transmission of the network. Here end to end delay increases. Also even if the node was found misbehaving this scheme takes some time to exclude it from future transmission until the counter reaches the threshold value. During this time the misbehaving node can incooperate serious damages to the network.
2. TWOACK [10]: In order to overcome the drawbacks in watchdog, a new scheme was proposed that is TWOACK. This scheme overcome two problems of Watchdog scheme ie the receiver collision and limited transmission power. TWOACK scheme is designed to detect misbehaving links rather than misbehaving nodes.This is done by acknowledging every data packet which has transmitted over three consecutive nodes along the path from the sender node to the receiver node.Since the acknowledgments are transmitted after every two hop transmission it significantly increases the routing overhead and end to end delay.

3. AACK [4]: It is similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). It can significantly reduce overhead when compared with TWOACK.
4. EAACK [11]: is an efficient intrusion detection scheme designed for MANET's which is capable of detecting false misbehavior report, receiver collision and can resolve limited transmission power problem.

3. PROBLEM DEFINITION

MANET's have a distributed architecture and changing (dynamic) topology. Hence many of the traditional intrusion detection schemes which were developed for wireless network is not feasible for MANET's. So it is important to develop an intrusion-detection system (IDS) which is designed specifically for MANETs. Many of the existing intrusion detection schemes in MANET encounters a very high end to end delay.Here, the main aim is to develop an efficient intrusion-detection mechanism which generates a very low end to end delay and at the same time by improving the packet delivery ratio.

4. SCHEME DESCRIPTION

In MANET each node can act as a sender and as a receiver. The proposed scheme includes a security checking module in each node ,so that the node that act as sender initiates a security checking process. Once the security checking process is initiated, each node in MANET is responsible to discover a valid route to the destination. This security checking's done during the route discovery phase. Thus the valid route to the destination by excluding the malicious node is determined before the actual data transmission phase begins. This provides more security to the data transmission in MANET's. The proposed scheme thus significantly reduces the end to end delay and also improves the packet delivery ratio. This scheme is mainly designed for military based application were the communication range is limited.

Initialy a single node act as a leader node which is responsible for broadcasting the group id value to all the nodes in the communication range. The leader node is dynamically changed. Hence no fixed node act as a leader node for all the communication. Leader node keeps on changing for each communication. Thus it prevents adversary from learning the location of leader node. Distribution of group id allows only those nodes with valid groupid to take part in the communication. The route request packets send by the source can be read only by the nodes which have the correct group id value. This happens since the route request is being encrypted using the senders private key and then appended with the group id. So only if the group id matches the intermediate nodes are allowed to decrypt the received packet. In this way the valid route to the destination is determined by avoiding the malicious node. Further transmission of data packets are done by hashing (SHA 1) and RSA encryption. The algorithm of the proposed scheme is given below in Fig 2.

SHA 1 (Secure Hash Algorithm) [16] is being incooperated into this proposed scheme to perform hashing.SHA1is based on MD4 algorithm[16].This algorithm takes an input message with maximum size less than 2^{64} bits and generates an output of 160 bit message digest. SHA1 is stronger against brute force attack.It is also not vulnerable to crytptanalytic attack.

The security in MANETs is defined as a combination of schemes and systems which can ensure integrity ,confidentiality, availability ,authentication and nonrepudiation [1].Digital signature is a widely used approach to ensure integrity, nonrepudiation and authentication of MANETs.

Digital signature can be considered as a string value, which appends a digital message with the source entity, else it may associate an electronic analog value of a written signature [14].

Digital signature schemes are broadly classified into the following two types:

a. *Digital signature with message recovery*: This scheme does not require the original message for the verification of the signature. Only the signature itself is required. Examples include RSA(Rivest Shamir Adleman) [15].
b. *Digital signature with appendix*: Here the original message is required for the signature verification algorithm. Examples include DSA (digital signature algorithm) [14].

RSA encryption is used in this proposed scheme.RSA (Rivest Shamir Adlemn) [15]algorithm is the most widely accepted and implemented approach to public key encryption. In this scheme plaintext and ciphertext are block ciphers of size between 0 and n-1 for some integer n. The size of n is about 1024bits.The encryption and decryption in RSA can be briefly explained as below:For some plaintext A and ciphertext B:

$$B=A^e \bmod n \quad (1)$$

$$A=B^d \bmod n = (A^e)^d \bmod n = A^{ed} \bmod n \quad (2)$$

Here the value of n is known to both the sender and receiver, But the value of e is known only to the sender and the receiver only knows the value of d. The detailed description of RSA algorithm can be found in [18].

4.1 Simulation Scenarios

The proposed scheme was simulated on 2 scenarios as follows:

Scenario 1: In this scenario ,a basic packet dropping attack was simulated. Here the malicious node drops all the packet it receives.The purpose of this scenario is to test the ability ofthe proposed scheme to detect the malicious node before it starts attacking the network.

Scenario 2: In this scenario the proposed scheme was compared against the existing EAACK scheme.The performance of the two IDS was compared based on the following metrics:

1. Packet delivery ratio:is the ratio of the packets receved in the destination to the packets send by the source.
2. Routing overhead:is the overhead incurred by the routing protocols during the route discovery process.
3. End-to-end delay: is the time taken by a packet to reach the destination from the source.

The performance of the proposed scheme was then studied by varying the percentage of malicious node in the network.

4.2 Simulation Configuration

The simulation was conducted using Network Simulator 2.34(NS 2.34) environment on a platform with GCC 4.3 and Ubuntu 10.10.This system was executed on a laptop with Core i3 CPU and 8GB RAM.NS2.34 was chosen as the simulation tool for its flexibility and better simulation capability. The default configuration in NS2.34 include 50 nodes and flat space of size 670 * 670 m.The total number of nodes was adjusted to 100 and 150 to evaluate the performance of the proposed scheme. Both the 802.11 MAC and physical layers are included in the wireless extension in NS 2.34.UDP with a constant bit rate was implemented with a packet size of 512 B.

Step 1. Begin
Step 2. Initialize the nodes as follows
a. Leader node: (shares the key at initial time)
b. Normal node: (normal mobile node)
Step 3. Leader node initially broadcast the GroupID (GID) key to all the mobile node in the network.
Step 4. Normal node saves the groupid value into memory
Step 5. If the node has a valid GID
a. It can access the request Step
6. Else
a. Can't access the request
Step 7. If node (i) wants to communicate with another node(j) then do the following during the route discovery phase:
a. Node i generates the hash code(by SHA-1)
b. Encrypt (by RSA) that code with the private key of node i
c. Append the encrypted output with the route request and send it to the destination node
Step 8. Destination node can verify that encrypted message by using the public key and as well as group ID
a. if match
i. node j sending own code(appended with route response) to source node i
b. if not match
i. ignore
Step 9. If the code matches a. transfer the data
Step 10. Else
a. ignore
Step 11.Select a new leader node after the current data transfer between the nodes get completed.
Step 12 .Dynamicaly generate a new Group id value by the new leader node and broadcast it to all the nodes in the network.
Step 13.Repeat the step 7 to step 10 for data transfer between any two nodes in the network.
Step 14.End

Fig-1: Algorithm of the proposed scheme

5. PERFORMANCE EVALUATION

The detailed simulation result are provided in Table 1 , Table 2, Fig 1 and Fig 2.

1. *Scenario 1*: In this scenario EAACK scheme was not capable of detecting malicious node before starting the communication through this node. The nodes were detected misbehaving by the EAACK scheme only after a delay. Thus the nodes could attack the network during this delay. But the proposed scheme was capable of detecting the malicious node before the node starts attacking the network. This is due to the security checking done during the route discovery process.

Table-1: Performance comparison based on packet delivery ratio

Percentage of malicious node	Proposed scheme	EAACK scheme	TWOACK scheme
10	83.00	79.21	68.89
20	86.38	72	64.71
40	94.21	76.77	70.55
60	86.28	68.80	56.73
80	88.91	68.26	55.23
90	67.45	65.21	43.89

Table-2: Performance comparison based on end to end delay

Percentage of malicious node	EAACK scheme	Proposed scheme
10	123.69	457.50
20	163.67	472.45
40	96.45	386.77
60	118.20	468.80
80	109.42	478.26
90	112.56	565.21

2. *Scenario 2*: In this scenario the performance comparison of the proposed and EAACK scheme was done. The proposed scheme was capable to offer an improvement in the packet delivery ratio than the EAACK scheme. This was possible because the proposed scheme only transmits the data packets only through the nodes that are trustworthy. The packet delivery ratio values obtained are shown in Table 1.

The proposed scheme encounters a very low end to end delay. Since the security checkings are done before the data transmission ,the packets are being transmitted at a very fast rate thus delay encountered in packet transmission is lowered. The comparision of the two schemes based on end to end delay metric is shown in Table 2.The proposed scheme encounters more routing overhead than the EAACK scheme since more security checkings are done during the route discovery process before selecting a particular path for data transmission. The comparision between the 2 schemes are shown in Fig 3 and Fig 4.

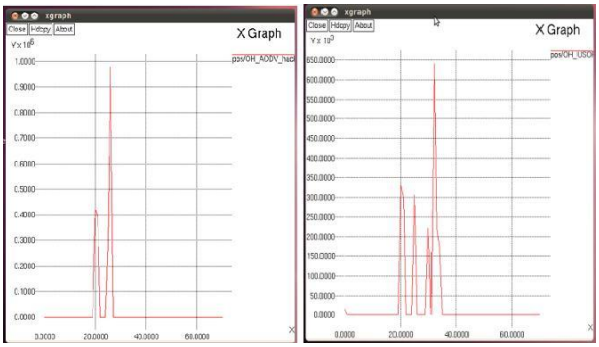

Fig-3: Routing overhead comparision, A)EAACK scheme B)Proposed scheme

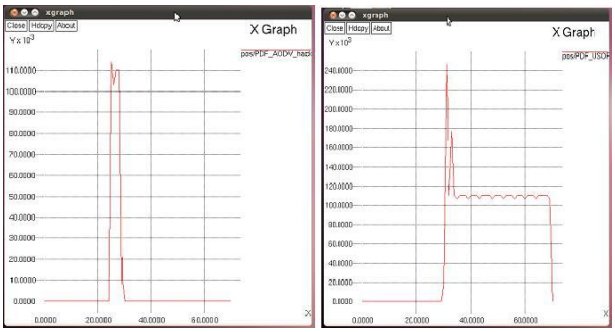

Fig-4: Packet delivery ratio comparision, A)EAACK scheme B)Proposed scheme

6. CONCLUSION

Due to extensive application in military, crisis management and in business environment, MANET have been an active field of research field over past few decades. The performance of this network to a great extend depends on the cooperation of all its member nodes. This property makes the network vulnerable to intrusions. In this paper an efficient intrusion detection scheme is proposed which offers anonymity to the nodes involved in the communication. The proposed scheme was capable of detecting the malicious nodes. It also improves the packet delivery ratio and significantly lowers the end to end delay. But this scheme encounters a high routing overhead. Hence we plan to focus the future research on issues such as adopting an efficient technique to reduce the routing overhead.Also testing of the proposed system in real-time environment is another area for future research.

REFERENCES

[1]. K. 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.NewYork: Springer-Verlag, 2012. pp. 659–666.

[3]. L. Zhou and Z. Haas, ―Securing ad-hoc networks, *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[4]. Y. Hu, D. Johnson, and A. Perrig, ―SEAD: Secure efficient distance Vector routing for mobile wireless ad-hoc networks,‖ in *Proc. 4th, IEEEWorkshopMobile Comput.Syst. Appl.*, 2002, pp. 3–13.

[5]. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, ―An acknowledgment-based approach for the detection of routing misbehavior in MANETs, *IEEE Trans.MobileComput.*, vol. 6, no. 5,pp. 536–550, May 2007.

[6]. J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, ―On intrusion detection and response for mobile adhoc networks in Proc IEEE Int Conf. Perform., Comput., Commun., 2004, pp. 747–752

[7] J.-S. Lee, ―A Petri net design of command filters for semiautonomous mobile sensor networks,‖ *IEEE Trans.Ind.Electron.*, vol. 55, no. 4, pp.1835–1841, Apr. 2008.

[8]. Denis Dondi, Alessandro Bertacchini, Davide Brunelli,,Luca Larcher and Luca Benini.*"*Modeling an Optimization of a Solar Energy Harvester System for Self-Powered Wireless Sensor Networks‖.

[9]. N. Nasser and Y. Chen, ―Enhanced intrusion detection systems for Discovering malicious nodes in mobile ad hoc network,‖in*Proc.IEEE Int.Conf. Commun.*, Glasgow,Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[10]. R. Rivest, A. Shamir, and L. Adleman, ―A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, vol. 21, no.2, pp. 120– 126, Feb. 1983.

[11]. Kasyap Balakrishnan Jing Deng Pramod KVarshnet TWO mACK:preventing Selfishness In Mobile Ad Hoc Networks, *IEEE Trans.MobComput*.2007.

[12]. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek, R.Sheltami ―EAACK—A Secure Intrusion-DetectionSystem for MANETs‖, Member, IEEE.

[13]. T.Sheltami, A. Al-Roubaiey, E. Shakshuki, and A.Mahmoud, ―Video Transmission enhancement in presence of misbehaving nodes in MANETs‖, *Int. J. Multimedia Syst.*,vol. 15, no. 5, pp. 273–282,Oct 2009.

[14]. Nat. Inst. Std. Technol., Digital Signature Standard (DSS Federal Information Processing Standards

Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).
[15]. R. Rivest, A. Shamir, and L. Adleman, ―A method for obtaining digital signatures and public-keycryptosystems,‖ *Commun. ACM*, vol. 21, no. 2,pp. 120 126, Feb. 1983.
[16]. Stéphane Manuel. Classification and Generation of Disturbance Vectors For Collision Attacks againstSHA1‖,IJCRT,2011.

BIOGRAPHIES

Renjini Rajendran is a MTech Student at Adi Shankara Institute of Engineering and Technology, Kalady in Mahatma University, Kottayam. Her interest areas include Network Security.

Ragesh G. K is an Assistant professor at Adi Shankara Institute of Engineering and Technology, Kalady in Mahatma Gandhi University