An Enhanced Scheme to Pinpoint Malicious Behavior of Nodes In Manet's

N.Malathi[1], Dr.M.Sivaram[2]

[1] *Post Graduate scholar, Department of Computer science and Engineering, Selvam College of technology, Tamil nadu, India*

[2] *Professor, Department of Computer science and Engineering, Selvam College of technology, Tamil nadu, India*

Abstract - *Mobile Ad hoc Network (MANET) has been pervasive in many applications, including some procedures such as security in critical applications has been a major threats in MANETs. This exceptional characteristic of MANETs, anticipation methodologies lonely cannot able to secure the data. In this circumstance secure acknowledgment of each data should have a defensive force before the attackers violate the system. The mechanism of Intrusion Detection System (IDS) is normally used to protect the wireless networks for security purposes in MANETs. In case of MANETs, intrusion detection system is favored since the first day of their invention.*

Keywords: Enhanced Adaptive Acknowledgement (EAACK), Digital signature,DSA,RSA

1. INTRODUCTION

Mobile Ad hoc Network is a mobile node with decentralized infrastructure services and self-configuring networks. The each mobile node is constructed with a wireless data transmitter and receiver that permit to communicate with radio frequency range. In these radio frequency ranges that supports the nodes in the wireless networks for secure acknowledgement in data transmission. MANETs usually consists of single hop data transmission and multi hop transmission of data. The nodes that communicates with one another in a radio frequency range is known as single hop data transmission and the nodes relay on another node when it is out of range in radio frequency is known as multi hop data transmission. In this data transmission, it may be text, picture, audio and video formats in the autonomous topology. A MANET with the characteristics described above was originally developed a research for military purposes, as nodes are spread across a battlefield and there is autonomous topology with decentralized infrastructure in networks. These MANETs are mainly used for military purpose for communication some examples are laptops, PDA or other mobile devices share wireless medium and communicate to each other.

The mechanism by which this is realized is called an Intrusion Detection System (IDS) for wireless MANETs. An IDS collects activity information and then analyzes the performance to determine whether there are any activities that violate the security rules [1]. Therefore, those techniques must be modified or new techniques must be developed to make intrusion detection work effectively in MANETs [9].

1.1 INTRUSION DETECTION SYSTEM IN MANETS

An IDS is used to protect the mobility of nodes to enhance the performance of network architecture. The most limitations of MANETs routing protocols, nodes in MANETs believe that other nodes must compromised with each other and relay on each nodes for data transmission [6]. IDS is mainly acts as the second layer in network layer that ensures the MANETs and its protocol [3]. An ID gives the Media Access Control (MAC) for transmission of data in the form of frames in a secure channel for addressing in communication range

1.2 Watchdog Approach

A Watchdog is an approach that secures the protection of MANETs IDS in network layer. Watchdog mainly ensures to improve throughput of network performance with the presence of malicious nodes. The protocol of Watchdog consists of two methods, namely Watchdog scheme and Path rater scheme. Watchdog scheme protects the IDS mechanism for MANETs, capable of identifying malicious nodes misbehaviors in the network. This further detects malicious misbehaviors by dissolutely listening to its next hop's transmission. If Watchdog node overhears in a network that will make failure count of the mobility of nodes [13]. This increases its failure counter of packets while transmitting and receiving the nodes. This increases its failure counter of packets while transmitting and receiving the nodes. Whenever a node is failure while transmitting and receiving at a certain threshold value, it reports to Watchdog and it verifies as a misbehaving node in network. In this method, Path rater scheme will identifies the misbehaving nodes in the form of failure count and reports to Watchdog scheme for future transmission [2] [3] [4]. This gives more advantages in reporting the misbehaving nodes, hence Watchdog is popular in some cases

1.3 Receiver collision

In this example of receiver collisions in MANETs, S is a source node and D is a destination node respectively, node A, B, C, X are the intermediate nodes between S and D nodes. When A sends a packet 1 to neighbor node B and it overhead occurs to forwarding the packets to node C successfully and failed to resemble the packet 1. When node C is already receiving a packet 2 from X node that causes a receiver collision to the destination node D.

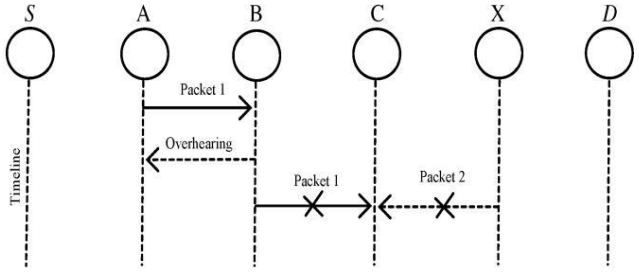

Fig.1 Receiver Collisions in both B and X node are trying to send packets to C node at the same instance of time

1.4 False misbehavior report

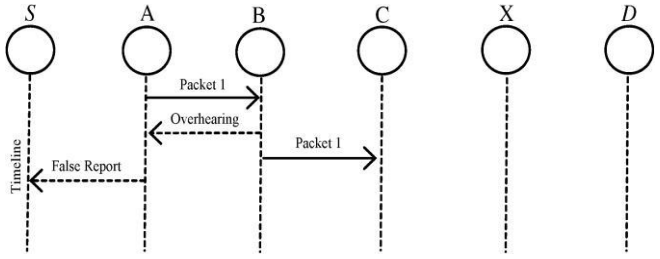

Fig.2 Node A sends back a misbehavior report even though node B forwarded the packet to node C.

For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, node A still reported node B as misbehaving, as shown in Fig. 2. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack.

1.5 Limited transmission power

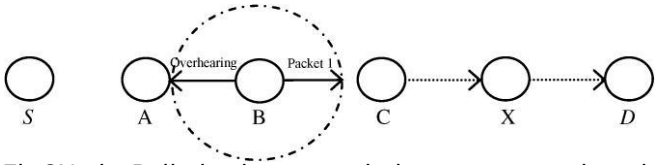

Fig.3Node B limits its transmission power so that the

packet transmission can be overheard by node A but too weak to reach node C.

In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C, as shown in Fig.3.

2. PROBLEM IDENTIFICATION

2.1 TWOACK

TWOACK is targeting to resolve the receiver collision in MANETs and limited transmission power problems of Watchdog method in IDS [10].TWOACK is a procedure to detect the misbehavior node. This is on retrieval of a packet in each node along the path requires acknowledgement nodes that is to hops away from the down of the route. TWOACK is mainly works on the principle of Dynamic Source Routing protocol.

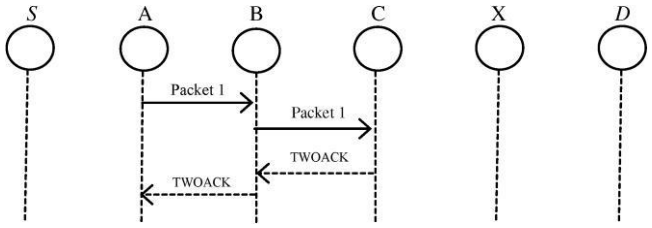

Fig.4. each node is required to send back an acknowledgment packet to the node that is two hops away from it.

2.2 AACK

AACK (Adaptive Acknowledgement) is based on TWOACK and it is research work, we analyze the digital signature to prevent from the attacker by forging acknowledgement packets. This usually finds the misbehaving nodes in a wireless network and gives more advantages than the TWOACK scheme. This will assign a throughput value for each failure nodes in a network and it will not all while acknowledgement in future transmission of data in each nodes.

3. SCHEME DESCRIPTION

In this scheme description, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA and RSA digital signature [11] schemes. EAACK is an acknowledgment-based IDS all three parts of EAACK, namely ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. The goal is to find the most optimal solution for using digital signature in MANETs and hybrid cryptographic key exchange algorithm is also used to reduce the network overhead.

3.1 ACK

ACK acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In Fig. 7, in ACK mode, node S first sends out an ACK data packet P_{ad1} to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives P_{ad1} , node D is required to send back an ACK acknowledgment packet P_{ak1} along the same route but in a reverse order. Within a predefined time period, if node S receives P_{ak1} , then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

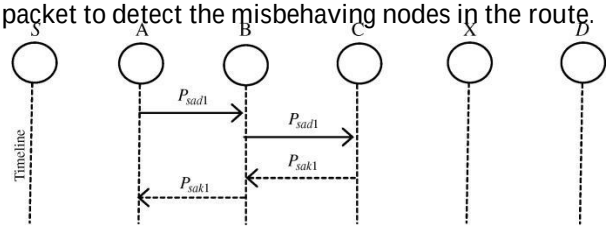

Fig.5.The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

3.2 S-ACK

This S-ACK scheme is a subjected to an updated scheme for TWOACK scheme [7]. The principle is usually allow every three consecutive nodes work in a network domain to achieve the threated misbehaving nodes. In this each and every three consecutive nodes that should be in a path, then third node is required to send an S-ACK acknowledgment packet to the first node. The S-ACK mode is to detecting misbehavior nodes in the presence of limited transmission power or receiver collision.

3.3 MRA

The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme [5] is to authenticate whether the destination node has received the reported missing packet through a different route between two nodes.

By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

3.4 DSA/RSA

EAACK has three parts namely, ACK,S-ACK,MRA are acknowledgement based detection schemes. They all relay on acknowledgement packets to detect misbehavior in the network. Thus it is extremely important to ensure that all acknowledgement packets in EAACK are authentic and untainted otherwise, if the attackers are smart enough to forge acknowledgement packets, all of the three schemes will be vulnerable. With regard to this urgent concern, in proposed to corporate digital signature. In order to ensure the integrity of IDS,EAACK requires all acknowledgement packets to be digitally signed before they are sent out and verified until they are accepted.1024 bit DSA key and 1024 bit RSA key has been generated for every node in the network. Both a public key and private key distributed in advance. The typical size of public and private key are 654b and 509b with 1024 DSA key and public key, private key of 1024 RSA key are 272b and 916b.The signature size of RSA and DSA are 89B and 131B.DSAscheme always produce less network overhead than RSA and the signature size of DSA much smaller than the signature size of RSA.Routing Overhead (RO) differences between RSA and DSA schemes vary with different number of malicious nodes. More number of malicious nodes requires no acknowledgement packets, thus increasing the ratio of digital signature in the whole network overhead.DSA requires more battery power than RSA. Considering the tradeoff between battery power and performance, DSA is still preferable

3.5 Hybrid Cryptographic Key Exchange Algorithm

Hybrid Cryptographic key exchange algorithm uses asymmetric key such as it may use public key as well as private key in a communication network to exchange request and response .The Key distribution is an important feature of predictable algorithm and the entire protection is needy on the distribution of key using secured channel[15].

HYBRID Cryptographic mechanism [11] utilizes the public and private key of asymmetric key cryptography to exchange the secret key to secure the information.

Define primitive root of a prime number 'm' as one whose powers generate all the integers from 1 to i-1, i.e. if 'a' is the primitive root of a prime no 'm', then, a mod m, a2 mod m, a 3 mod m, am-1 mod m generate all distinct integers from 1 to (m-1) in some permutation.

The steps for HYBRID key exchange algorithm are given as: Step 1: The GLOBAL PUBLIC KEY ELEMENTS Choose any prime no: 'n'

Calculate the primitive root of n: 'a' such that a<n. Step 2: An ASYMMETRIC KEY GENERATION MECHANISM BY

USER 'A'

Choose a random number as the private key element XA Where XA< n

Then calculate the public key YA where YA = a. XA modn Step 3: The KEY GENERATION BY USER B Choose a random number for a Private Key B

Where XB< n

Then calculate the public key YB where YB = aXB mod n Step 4: We need to exchange the values of public key generation between A &B

Step 5: We Choose a SYMMETRIC KEY

(K) GENERATION BYUSER 'A'
K= YB XA mod n

Step 6: We choose a SYMMETRIC KEY (K) GENERATION BYUSER 'B'

K= YA XB mod n

This means that all numbers k=1, .. m-1 can be represented as k= gi

For example, X=gx mod m

2. Bob selects a large random number y and requests Alice Y=gy mod m
3. Alice computes k=Yx mod m

Bob computes k=Xymod

4. CONCLUSIONS

In this secure authentication method, hybrid cryptographic techniques is specially designed for MANETs and reduce the network overhead in mobile nodes. It establishes and ensures the higher misbehavior reports to increase the network performance while acknowledging the packets in EAACK scheme. So this approach of hybrid cryptographic mechanism leads to reduce in network overhead in autonomous topology.

ACKNOWLEDGEMENT

We feel greatly indebted to express my sincere gratitude to our Dr.Sivaram..Ph.D for providing us the necessary facilities for the completion of this paper.

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. 659–666R

[2] H. Akbani, S. Patel, and D. C. Jinwala, "*DoS attacks in mobile ad hoc networks: A survey,*" in Proceedings in 2nd International Meeting AC CT , Rohtak, Haryana, India,2012, pp. 535–541

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

[4] N. Kang, E. Shakshuki, and T. Sheltami, "*Detecting misbehaving nodes in MANETs,*" in Proceedings in 12th International Conference WAS, Paris, France, Nov. 8– 10,2010, pp. 216–222

[5] N. Kang, E. Shakshuki, and T. Sheltami, "*Detecting forged acknowledgements in MANETs,*" in Proceedings IEEE 25th International Conference AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494

[6] Tabesh and L. G. Frechette, "*A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micro power generator,*" IEEE Transaction Industrial Electronics, vol. 57, no. 3, pp. 840–849, Mar. 2010.

