An Enhanced Timer-ACK Scheme using Hybrid Cryptography for Misbehavior Node Detection in MANET

Remya P V, *PG Scholar*
Department of Computer Science & Engineering, Malabar Institute of Technology
Anjarakandy, Kannur (Dt), Kerala

Rijin I K, *Faculty*
Department of Computer Science & Engineering, Malabar Institute of Technology
Anjarakandy, Kannur (Dt), Kerala

Abstract **- Mobile Ad-hoc network (MANET) is network consisting of setting mobile nodes allied with wireless links. Since it is infrastructure less pattern, it is highly exposed to attacks due to the dynamically altering network topology, deficit of centralized monitoring and open medium. Therefore an intrusion detection system (IDS) is necessitated that monitors the network, detects misbehavior or inconsistency and inform other nodes in the network to avoid the misbehaving nodes. The existing IDS plan is Enhanced Adaptive ACKnowledgment (EAACK), designed to tackle three delicacy namely, false misbehavior, limited transmission power, and receiver collision. EAACK consist of three major parts, namely, Acknowledgement-ACK (reduces network overhead), secure Acknowledgement (S-ACK, to observe misbehaving nodes), and misbehavior report authentication (MRA, to identify the residence of false misbehavior report).This scheme also subsume digital signature, in order to certain the integrity of the IDS. The proposed scheme- An enhanced Timer based Acknowledgement scheme using hybrid cryptography is an expanded version of EAACK. EAACK cause more routing overhead due to digital signature when there are more malicious nodes with acknowledge packets. So the hybrid cryptography method is used to reduce the network overhead caused by digital signature. Also a timer based acknowledgement approach added in with S-ACK mode. There is no need to transmit acknowledgement for reception of each data packet since it is processed in group wise and it decreases the waiting interval for acknowledgement and also overhead is narrowed.**

Keywords— Mobile Ad hoc Network (MANET); Intrusion detection; Cryptographic algorithms; Hybrid cryptography; Digital signature;

I. INTRODUCTION

Mobile Ad hoc networks or MANETs are the class of wireless networks which do not necessitate any fixed infrastructure or base stations. They can be easily deployed in areas where it is strenuous to setup any wired infrastructure. With the improved technology and reduced costs, wireless networks have gained consideration over wired networks in the past few decades. MANET is a collection of mobile nodes with both a wireless transmitter and receiver that communicate with each other through bidirectional wireless links. MANETs have applications in several areas like in military applications where relaying important data of situational consciousness on the battleground, in corporate houses where employees sharing information inside the company premises or in a meeting hall attendees using wireless gadgets participating in conference, critical mission programmer for matters in any disaster events like large scale like war or terrorist attacks, natural disasters and all ([1],[2]). Routing protocols does two important functions Routing function and Data-Forwarding function. Both would be affected with the existence of misbehaving nodes. Node's misbehavior can be classified [3] as malfunctioning, selfish or malicious nodes. Malfunctioning nodes suffer hardware failures or software errors. Selfish nodes refuse to forward or drop the data packet. It can take part in the route discovery and route maintenance stages but refuses to forward data packets to save resources. Malicious nodes use their resource and aims to drop other nodes or whole network by trying to participate in all, established routes and forcing other nodes to use a malicious route which is under their control. Unfortunately, the open medium and remote distribution of MANET make it exposed to various types of attacks. For example due to the nodes absence of physical security, malicious attackers can easily find and compromise nodes to achieve attacks. In such case, it is important to develop an intrusion-detection system (IDS) specially designed for MANETs.

A. Background

1) Intrusion Detection System (IDS) in MANET

Intrusion is any set of actions that try to compromise the integrity, confidentiality or existence of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions. There are three main components of IDS: data collection and responses. The data collection component is responsible for collection and pre-processing data tasks: transferring data to a common format, data storage and transmit data to the detection module. IDS can use different data sources as inputs to the system: system logs, network packets, etc. In the detection component data is analyzed to detect intrusion attempts and indications of detected intrusions are sent to the response component.

2) Cryptographic algorithms

The cryptographic algorithms are classified into two different methods such as symmetric and asymmetric method. In symmetric encryption, a key is shared between the sender and the receiver which is kept secret from the intruder. Among the various kinds of symmetric algorithms, Advanced Encryption Standard (AES) is gaining popularity due to its better security and efficiency than its predecessors.

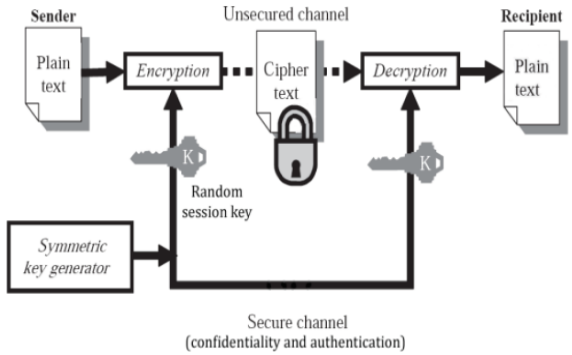

Figure 1: Symmetric cryptography

Asymmetric cryptography uses a pair of keys to encrypt and decrypt message. One key is known as public key as it is distributed to others and the other is called private key which is kept secret. Usually public key is used to encrypt any message which can only be decrypted by the corresponding private key. RSA is the most widely used asymmetric encryption system which was invented by Ronald Rivest, Adi Shamir, and Len Adleman.

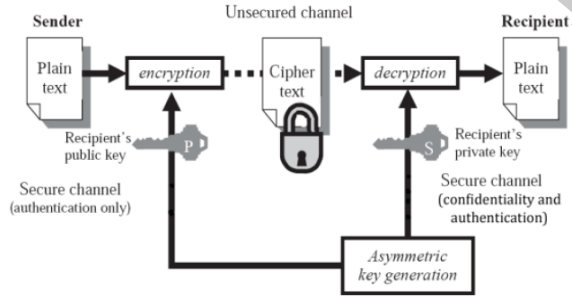

Figure 2: Asymmetric cryptography

3) Digital Signature

Digital signatures have always been an integral part of cryptography in history. It is an authentication mechanism that enables the creator of a message to attach a code known as signature which is formed by taking the hash of the message and encrypt using creator's private key. Digital signature schemes can be mainly divided into the following categories.

- Digital signature with appendix: The original message is necessitated in the signature verification algorithm. It includes a digital signature algorithm (DSA).
- Digital signature with message recovery: This type of scheme does not necessitate any other information besides the signature itself in verification process. Examples include RSA.

4) Hybrid cryptography

Hybrid cryptography [4] is a mode of encryption/decryption that merges two or more cryptographic systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are uniquely defined as speed and security. Since AES provides better security and has less implementation complexity, it has come up as one of the strongest and most effective algorithms in existence today. RSA solves the problem inherent distributing the secret key. So we can conclude in hybrid approach we can use AES & RSA

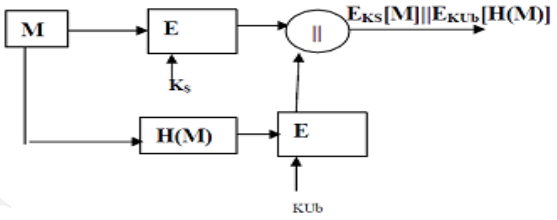

Figure 3: Hybrid encryption

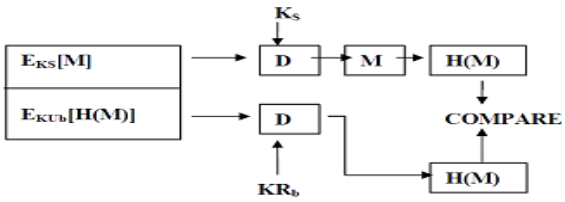

Figure 4: Hybrid decryption

II. RELATED WORK

IDSs usually act as the second layer in MANETs, and they are a great helpful in existing proactive approaches Anantvalee and Wu [5] presented a very thorough survey on contemporary IDSs in MANETs. In this section, we describe existing approaches, namely, Watchdog, TWOACK, and EAACK

A. Watchdog

Marti et al. [6] Watchdog aims to improve throughput of network with the existence of malicious nodes. The watchdog scheme is of two parts, namely Watchdog and Pathrater. It provides as an intrusion detection system for MANETs. It is responsible for finding malicious nodes misbehaviors in the network. Watchdog finds malicious misbehaviors by promiscuously listening to next hop's transmission. If Watchdog node overhears that its next node fails to forward the packet within a certain period, it increases failure counter. When a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the

Pathrater along with the routing protocols to avoid the reported nodes in future transmission. Most following researches and implementations have proved that the Watchdog scheme to be efficient. To add on, compared to some other schemes, Watchdog can detect malicious nodes rather than links. These advantages have made Watchdog scheme a popular choice in the field. Many MANET IDSs are developed as an improvement to the Watchdog scheme. Watchdog method fails to detect malicious misbehaviors with the existence of ambiguous collisions, limited-transmission power, false misbehavior report, receiver collisions, collision and partial dropping.

B. TWOACK

TWOACK proposed by Liu et al. [7] is one of the most important approaches among them. TWOACK is neither an enhancement nor a Watchdog based method. Targeting to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK finds misbehaving links by acknowledging all data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each of nodes along the route is necessitated to send back an acknowledgement packet to the node that is two hops away from it down the route.

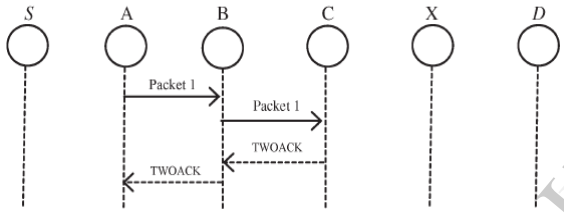

Figure 5: TWOACK scheme

C. EAACK (Enhanced Adaptive Acknowledgement)

Proposed by Elhadi & Sheltami [8] designed to tackle three of the six weaknesses of Watchdog scheme false misbehavior, receiver collision and limited transmission power. Furthermore, they extend their research to adopt a digital signature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is vital to ensure the integrity and authenticity of all acknowledgment packets. So the introduction of digital signature, prevent the attacker from forging acknowledgment packets.

D. TimerACK

Proposed by Ramasamy Murugan and Arumugam Shanmugam[8] for detecting selfish nodes which drop packets such that the other nodes can never use it. Here the selfish behavior of the nodes is considered as misbehaving because they drop packets to save battery power. In order to track the incoming packets and outgoing packets a forward counter Fc is used in each node. The forward counter is updated when a packet leaves the node and when a packet enters the node. A detection timer Dtimer is assigned for every group of nodes with specific time period. When Dtimer starts the source node, i.e FNode starts forwarding the packets and when the Dtimer expires, the last node tell LNode send as acknowledgement to SNode.

III. PROBLEM IDENTIFICATION

The existing scheme implemented both DSA and RSA in EAACK scheme. The DSA propose always produces slightly less network overhead than RSA does. This is easy to find because the signature size of DSA is much smaller than the signature size of RSA. However, it is interesting to observe that the RO differences between RSA and DSA schemes vary with different numbers of malicious nodes. More malicious nodes there are more ROs the RSA scheme produces. We assume that this is due to the fact that more malicious nodes necessitate more acknowledgment packets, thus increasing the ratio of digital signature in the whole network overhead. Many of the existing IDSs in MANETs adopt an acknowledgment based scheme, including EAACK. The functions of this detection scheme largely depend on the acknowledgment packets. So, it is guarantee that acknowledgment packets are valid and authentic by using digital signature.

Sending of acknowledgement packets and counting the number of data packets individually is time consuming. Digital signature cause routing overhead when more no. of malicious nodes present. The process is always accompanied with delay. In this research work, our goal is to propose a IDS specially designed for MANETs, which solves receiver collision, limited transmission power and mainly false misbehavior report and routing overhead caused by digital signature but also improve the security in system.

IV. PROPOSED MODEL

The approach described in this research paper is based on the previous work-EAACK. In this paper, we extend it with the introduction of enhanced timer based acknowledgement scheme (TimerACK) and hybrid cryptography.

First find out a secure route for data transmission using Dynamic Source Routing Protocol (DSR). Enhanced TimerACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet in different schemes, we included a 2-b packet header. According to the Internet draft of DSR, holds 6 b reserved in the DSR header. There are some assumptions in order for TimerACK to work

1. Link between each node in the network is bidirectional.
2. For each communication process, the source node and destination node are not malicious. Else specified, all acknowledgment packets described in this research are necessitated to be digitally signed by its sender and verified by its receiver.

A. ACK

ACK is basically an end-to-end acknowledgment scheme. It shows as a part of the hybrid scheme, aiming to reduce network overhead when no network misbehavior is detected. In Fig. 2, in ACK mode, node S first sends out an ACK data

packet Pad1 to the destination node D. If all the intermediate nodes with the route between nodes S and D are cooperative and node D successfully receives Pad1, node D is necessitated to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order. Within a predefined time interval, if node S receives Pak1, then the packet transmission from node S to node D is successful. Else, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

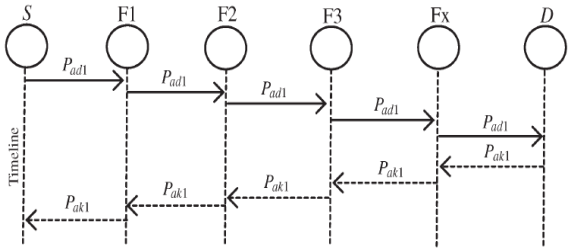

Figure 6: ACK scheme

B. S-ACK

It is assumed that, each node maintains a LIST which contains ID of every data packets sent or forwarded. This scheme involves 3 steps.

1) Grouping of Nodes

As soon as the desired route is found, all the nodes of the desired route are logically grouped into N sets (i.e.M1, M2, M3…Mn), where M=m/3 (m is the number of nodes in the desired route) such that the group M1 contains first three consecutive nodes and group M2 contains next three consecutive nodes (as in Figure 4.2) and so on. Hence a group M1 consists of the source S which is First node referred as FNode and the intermediate node referred as INode and the Last node of the group is referred as LNode. For eg. if S->R1->R2->R3->R4->R5->R6->R7->D is the desired route then nodes of the desired path forms three groups (i.e M1, M2, M3).

The Group M1=S->R1->R2

Group M2=R3->R4->R5

Group M3=R6->R7->D

The proposed work focuses on detecting selfish nodes which drop packets such that the other nodes can never use it. Here the selfish behavior of the nodes is considered as misbehaving because they drop packets to save battery power. In order to track the incoming packets and outgoing packets a forward counter Fc is used in each node. The proposed work focuses on detecting selfish nodes which drop packets such that the other nodes can never use it. Here the selfish behavior of the nodes is considered as misbehaving because they drop packets to save battery power. In order to track the incoming packets and outgoing packets a forward counter Fc is used in each node. The forward counter is updated when a packet leaves the node and when a packet enters the node. A detection timer Dtimer is assigned for every group of nodes with specific time interval. If when Dtimer starts the source node, i.e FNode starts forwarding the packets and when the Dtimer expires, the last node say LNode send as acknowledgement to the SNode.

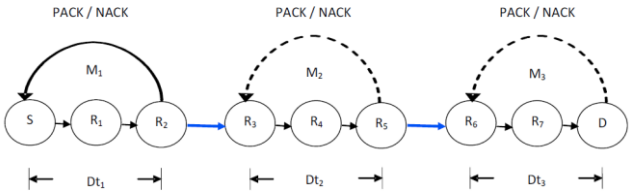

Figure 7: S-ACK scheme using timer

2) Detecting Misbehaving Nodes

The nodes start forwarding the packet upon request. When this action begins, the D timer starts. The forward counter is on and this gets incremented or decremented according to the flow. When the packet enters the node, the Fc is incremented and when the packet leaves node Fc is incremented. After the Dtimer expires, the last hop node of the group compares the value of Fc with forward counter threshold Fct. If Fc of LNode is equal to Fct then PACK is sent else NACK is sent (as in fig.3). In this manner the process continues for every group of nodes.

All the three schemes are acknowledgement based detection schemes. It is extremely important to ensure that all packets are digitally signed. Therefore ACK packet is encrypted using RSA & AES (hybrid approach). Before receiving, it will be decrypted.

3) Mitigating Misbehaving Nodes

If the source is informed with PACK, the route is considered as normal. If NACK is informed to the source node, then the source node of every group counts the NACK of each node. If NACKc is greater than NACKcmax, then the node is considered as misbehaving and this information is broadcasted to all other groups in the route. Also a misbehavior report will be generated by node and sent to source node then switch to MRA scheme.

C. MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the existence of false misbehavior report. The wrong misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be poison to the entire network when the attackers break down sufficient nodes and thus cause a network division. The key of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the

destination node. If there is no other that present, the source node will starts a DSR routing request to find another route when the destination node receives an MRA packet, it finds in its local knowledge base and compares if the reported packet was received. If already received, then safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Else, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, TimerACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

V. ADVANTAGES/ DISADVANTAGES

Advantages;

1) Solves limited transmission power and receiver collision problem: - since the proposed model uses S-ACK mode for this.
2) Capable of detecting misbehavior attack with the help of S-ACK & MRA
3) Ensure authentication and packet integrity using hybrid cryptography
4) Digital signature prevents the attack of forge acknowledgement packets.
5) Reduces routing overhead due to digital signature by using hybrid cryptography
6) Minimizes waiting period for acknowledgement since it is processed in group wise

Disadvantages;

- Absence of central points:

MANET do not have an entry points such as routers or gateways. A node can send or receive packet within its radio range. But IDS needs to be distributed and co-operative. This make IDS agent strenuous in an environment where resources like bandwidth, processor speed are limited.

- Absence of clear line of defense and secure communication

MANET do not have clear line of defense, attacks can come from all directions. For instance there are no central points on MANET where access control mechanisms can be placed.

- Cooperativeness:

MANET routing protocols are usually very cooperative. This would make them the target of new attacks.

VI. FUTURE SCOPE

Packet-dropping attack has always been a big threat to the security in MANETs. Although it generates more routing overhead in some cases, we think that this condition is worthwhile when network security is the top priority. Furthermore, in an effort to prevent the intruders from initiating forged acknowledgment packets,

To increase the advantages of our research work, we propose to discover the following problems in our future research:

1) Observing the possibilities of adopting a key exchange mechanism to eliminate the necessitate pre distributed keys.

2) Testing the performance of TimerACK in real network environment instead of software simulation.

VII. CONCLUSION

In this paper, we propose an enhanced timer based acknowledgement scheme using hybrid cryptography that detects and isolates the misbehavior nodes in MANET. It consisted of three major parts, namely, ACK (reduces network overhead), secure ACK (S-ACK, to resolve receiver collision and limited transmission problem), and misbehavior report authentication (MRA, to identify the existence of false misbehavior report).This scheme also incorporated digital signature, in order to ensure the integrity of the IDS. There is no need of sending acknowledgement for reception of each data packet since it is processed in group-wise and it reduces the waiting period for acknowledgement and also overhead is reduced. Major threats like false misbehavior report and forge acknowledgement can be detected by using this scheme. But Packet-dropping attack has always been a big issue to the security in MANETs

REFERENCES

[1] 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, 2007 Jun. 24–28, pp. 1154–1159.

[2] M. Zapata and N. Asokan, Securing ad hoc routing protocols, in Proc. ACM Workshop Wireless Secur., pp. 1–10.2002

[3] S. Dhanalakshmi and M. Rajaram ,A reliable and secure framework for detection and isolation of malicious nodes in MANET, International Journal of Computer Science and Network Security, vol..8, no.10, pp. 184-190, 2008.

[4] Abdullah Al Hasib and Abul Ahsan Md. Mahmudul Haque-Helsinki University of Technology Telecommunication Software and Multimedia Laboratory Finland -A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography -Third International Conference on Convergence and Hybrid Information Technology 2008

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

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.2000

[7] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami (2013), EAACK—A Secure Intrusion-Detection System for MANETs, IEEE-IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013

[8] Ramasamy Murugan and Arumugam Shanmugam (2013) A Timer Based Acknowledgement Scheme for Node Misbehavior Detection and Isolation in MANET.