Hybrid Cryptography Technique For Mobile Ad-hoc Network

M.sangeetha[1], V.Vidya Lakshmi[2]
PG Scholar, Department of ECE, Velammal Engineering College, Chennai, Tamil Nadu, India[1]
Assistant Professor II, Department of ECE, Velammal Engineering College, Chennai, Tamil Nadu, India[2]

Abstract— Computer today have a plethora of applications, spread over a wide spectrum. They are used in critical applications such as electronic fund transfer and storage of information in medical systems and so on. The level of security for particular systems depends on the resources being secured. Information in banking has a great financial value. Information in Medical system has life-or-death value. The information obtained may be of little value to the intruders but it could be a major embarrassment to the system administrator. Here breach in security however it cannot be ignored .The ultimate goal of proposed approach is to secure the data using HYBRID CRYPTOGRAPHY TECHNIQUE which has been invented to addresses the vulnerabilities in both proactive and reactive environment. The proposed scheme is based on parts, in which the data is encrypted and sent through unauthorized nodes then to the destination which will increase the quality of service by reducing the network traffic. This will add a new dimension of security to the entire network .This makes the security parameters known only to the server authenticating the nodes. Attackers would be unlikely able to know the private key and the encrypted data. Moreover this technique will avoid the routing overhead in both proactive and reactive environments and consequently speed up the secured delivery of data which is very critical to wireless technologies.

Index Terms—Mobile Ad-hoc Network,dynamic network,onion routing protocol, routing overhead.

I.INTRODUCTION

Mobile Ad Hoc network is a collection of wireless mobile terminals that are able to dynamically form a temporary network without any centralized administration. Such networks are characterized by: Dynamic topologies, existence of bandwidth constrained and variable capacity links, energy constrained operations and are highly prone to security threats. Due to all these features routing overhead is a major issue in ad hoc networks. The traditional routing protocols for MANETS undertakes set-up and maintain routes between nodes. The existing routing protocols may be categorized into Proactive ones and Reactive ones. e.g. Destination Sequenced Distance Vector (DSDV) , Optimized Link State Routing (OLSR), Reactive/On-demand, e.g. Dynamic Source Routing Protocol (DSR), Ad hoc On-Demand Distance Vector routing protocol (AODV), Temporally Ordered Routing Algorithm,

attempt to provide only best effort delivery. Their target is limited to finding the minimum hops or the shortest paths. In MANETS continuously changing network topology causes link breakage and invalidation of end-to-end route. The routing protocols need to resolve the link failure prediction and route recovery to adapt to dynamic change of network topology and thus to reduce routing overhead.

II. BACKGROUND

As discussed before, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, an IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches . Anantvalee and Wu [4] presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog [17], TWOACK [15], and Adaptive ACKnowledgment (AACK) .

1) Watchdog: Marti *et al.* proposed a scheme named Watchdog that 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 an 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. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, 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 .

The 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. We discuss these weaknesses
with further detail in Section III.

2) TWOACK: With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu *et al.* is one of the most important approaches among them.

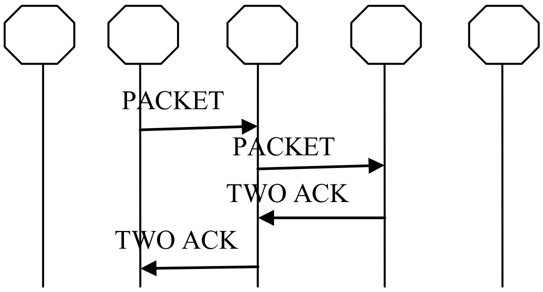


Fig.1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

On the contrary to many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) [11]. The working process of TWOACK is shown in Fig. 1: Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three consecutive nodes along the rest of the route.

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network. However, many research studies are working in energy harvesting to deal with this problem.

III. PROBLEM DEFINITION

A.HYBRIDCRYPTOGRAPHYTECHNIQUE is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, remove packet dropper ,nodes, and receiver collision. In this section, we discuss these three weaknesses in detail.

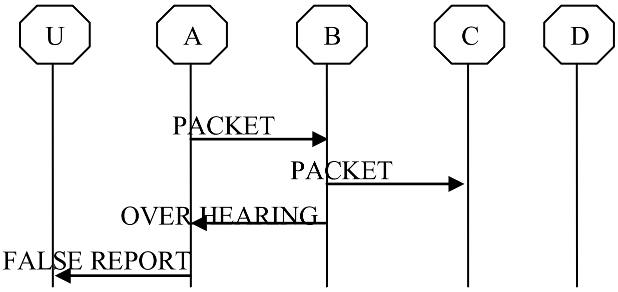


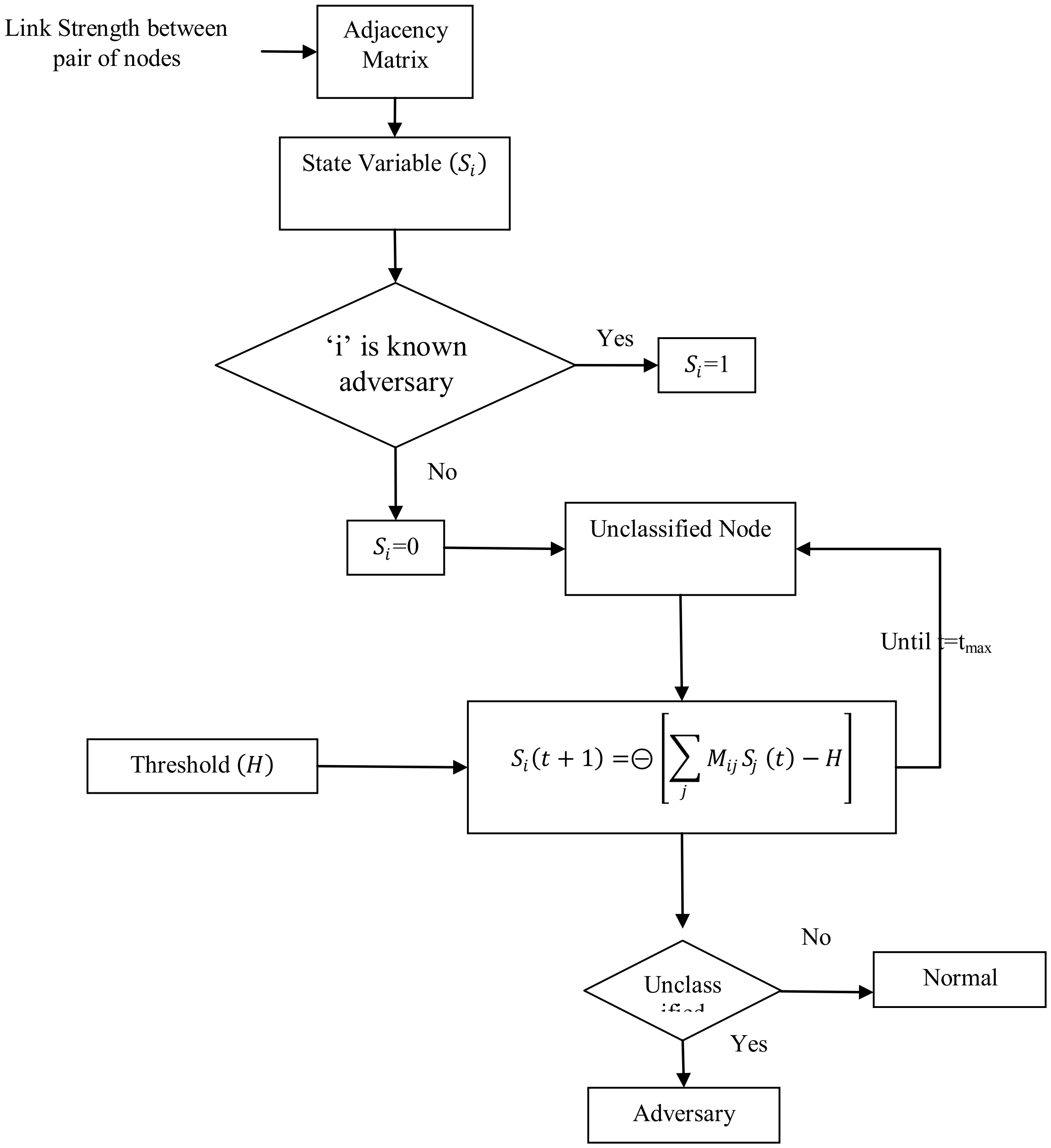
Fig. 2. False misbehavior report: Node A sends back a misbehavior report even though node B forwarded the packet to node C.

B. NODE CATEGORIZATION ALGORITHM

In every round, for each mobile node *u*, the destination keeps track of the number of packets sent from *u*, the sequence numbers of these packets and the number of flips in the sequence numbers of these packets, (i.e., the sequence number changes from a large number such as *Ns* ¡ 1 to a small number such as 0).In the end of each round, the destination calculates the dropping rate for each node *u*. Suppose *nu,* is the most recently seen sequence number, *nu, flip* is the number of sequence number flips and *nu, rcv* is the number of received packets. The dropping ratio in this round is calculated:

$$\frac{n_{u,flip} * N_s + n_{u,max} + 1 - n_{u,rcv}}{n_{u,flip} * N_s + n_{u,max} + 1},$$

D.ITERATIVE CATALOGGING ALGORITHM



IV ONION ROUTING PROTOCOL

AND TWO FISH ALGORITHM

A.ONION ROUTING PROTOCOL

Onion routing is a protocol used to communicate for secured transaction of data in the network.one of the best encryption technique that has been used to protect the data. It can transact the data using three layer key protections. In this protocol, the message is hidden and transmitted. It is a routing protocol technique anonymous communication over a computer network. The idea of onion routing is to protect the privacy between the sender and receiver on the computer network. It is an end-to-end communication service. Messages are repeatedly encrypted and then sent several network nodes. Onion accomplishes that the data travel from the sender to the receiver

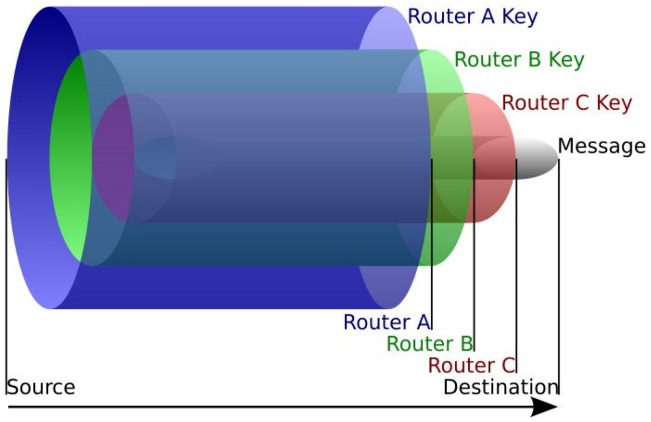
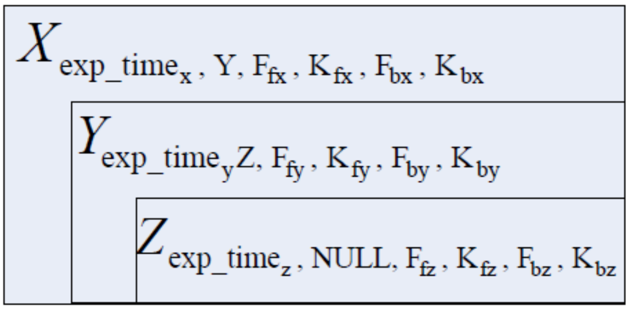


FIG 4. Structure of Onion routing protocol

The onion data structure is composed of layer upon layer of encryption wrapped around a payload. Leaving aside the shape of the payload at the very center, the basic structure of the onion is based on the route to the responder that is chosen by the initiator's proxy. Based on this route, the initiator's proxy encrypts first for the responder's proxy, then for the preceding node on the route, and so on back to the first routing node to whom he will send the onion.



$$X_{\text{exp\_time}_x,\ Y,\ F_{fx},\ K_{fx},\ F_{bx},\ K_{bx}}$$

$$Y_{\text{exp\_time}_y Z,\ F_{fy},\ K_{fy},\ F_{by},\ K_{by}}$$

$$Z_{\text{exp\_time}_z,\ \text{NULL},\ F_{fz},\ K_{fz},\ F_{bz},\ K_{bz}}$$

Fig 5 Structure of Forward Onion

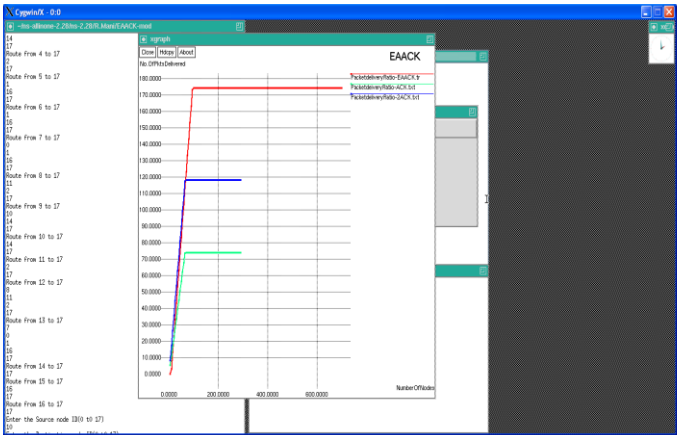
When the onion is received, each node knows who sent him the onion and to whom he should pass the onion. But, he knows nothing about the other nodes, nor about how many there are in the chain or his place in it(unless he is last). What a node Px receives looks like this.{exp_time,next hop, Ff, Kf, Fb, Kb, payload} PKx Here PKx is a public encryption key for routing node Px, who is assumed to have the corresponding decryption key. The decrypted message contains an expiration time for the onion, the next routing node to which the payload is to be sent, the payload, and two function/key pairs specifying the cryptographic operations and keys to be applied to data that will be sent along the virtual circuit. The forward pair (Ff, Kf) is applied to data moving in the forward direction. (Along the route the onion is travelling) The backward pair (Fb, Kb) is applied to data moving in an opposite direction (along the onions reverse route). (If the receiving node is the responder's proxy, then the next hop field is null). For any intermediate routing node the payload will be another onion. The expiration time is used to detect replace, which pairs of compromise nodes could used to try to correlate messages. Each node holds a copy of the onion until exp_time. If he receives another copy of the same onion within that time he simply ignores it. And, if he receives an onion that has expired, he ignores that as well.

V. SIMULATION RESULTS

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics .

1) *Packet delivery ratio (PDR)*: PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

2) *Routing overhead (RO)*: RO defines the ratio of the amount of routing-related transmissions



```
14
17
Route from 4 to 17
2
17
Route from 5 to 17
1
16
17
Route from 6 to 17
1
16
17
Route from 7 to 17
0
1
16
17
Route from 8 to 17
11
2
17
Route from 9 to 17
10
14
17
Route from 10 to 17
14
17
Route from 11 to 17
2
17
Route from 12 to 17
8
11
2
17
Route from 13 to 17
7
0
1
16
17
Route from 14 to 17
17
Route from 15 to 17
16
17
Route from 16 to 17
17
Enter the Source node ID(0 to 17)
10
```

Fig 6 Packet Delivery Ratio

VI CONCLUSION AND FUTURE WORKS

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets.We think that this tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs.

REFERENCES

[1] M. Sailaja, R. Kiran Kumar, P. Sita RamaMurty, and P E S N Krishna Prasad," A study on routing algorithm derived from nature of MANET" ,May2011.

[2]Ashish Kumar, Vidya Kadam, Subodh Kumar and Shital Pawar," An Acknowledgement-Based Approach for the Detection of Routing Misbehavior in MANETS", 2011.

[3]H Yang H Y. Luo F Ye S W. Lu L Zhang," Security in mobile ad hoc networks: Challenges and solutions",2004.

[4]Aravinth Raj, Shanmogavel, Avinash Mistry, Nitin Chander Prashanth, Patlolla, Vivek Yadlapalli" Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols",2007.

[5]Sofiane Hamrioui , Mustapha Lalam , Pascal Lorenz ,"Improving Acknowledgement Mechanism of TCP for better performance in MANET" ,2012.