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

Secure Data Transmission in MANETS Using ELIPTIC Curve Cryptography

K.Sangeetha[1]

M.E Computer and communication Engg, Department of I.T, SNS College of Technology, Coimbatore, Tamilnadu, India[1]

ABSTRACT: MANET is a collection of wireless mobile nodes forming a network without using any existing infrastructure. There are various challenges that are faced in the Adhoc environment. These are mostly due to the lack of resources of these networks. The solutions for conventional networks are usually not sufficient to provide efficient Adhoc operations. The wireless nature of communication and lack of any security infrastructure raise several security problems. Enhanced Adaptive Acknowledge (EAACK) one of the Intrusion Detection System (IDS) mechanism which increases the integrity IDS of using digital signature.ACK digitally signed before its reach destination. In EACCK chances to make false acknowledgement. EACCK uses DSR routing protocol for identifying the route.DSR causes more Routing Overhead. Instead of DSR, AODV is used for route discovery. AODV has potentially less routing overhead than other protocol and AODV route replies only carry the destination IP address and the sequence number. The advantage of AODV is that it is adaptable to highly dynamic networks. Eliptic curve cryptography (ECC) can be developed in order to make the path more secure and also used to eliminate the requirement of pre-distributed keys. Key exchange (also known as "key establishment") is a method by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt the messages received.

KEYWORDS: EACCK, AODV, DSR, IDS, ECC

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links both directly or indirectly. One of the foremost advantages of wireless networks is its ability to allow data communication between different users and still maintain their mobility. This communication is limited to the range of transmitters. The two nodes cannot communicate with each other when the distance between the two nodes is afar the communication range of their own. MANET solves this communication problem by allowing intermediate users to data transmissions. Allowing intermediate user is achieved by dividing MANET into two kinds of networks, namely, single-hop and multi hop. All nodes within the same radio range communicate directly with each other is called single-hop network. In a multi hop network, nodes rely on other intermediate users to transmit if the destination node is out of their radio range. In different to the traditional wireless network, MANET has a decentralized network infrastructure. In MANET all nodes are free to move randomly. MANET is capable of creating a Self-configuring and self-maintaining network without the help of a centralized infrastructure. MANET is popular among serious mission applications; network security is of vital importance. The open medium and remote distribution of MANET make it vulnerable to various types of attacks. Example, by reason of the nodes' lack of physical shield, malicious attackers can simply capture and compromise nodes to realize attacks. In particular, considering the fact that most routing protocols in MANETs

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

assume that every node in the network performs helpfully with other nodes and presumably not malicious [1], attackers can simply compromise MANETs by inserting malicious or non-co-operative nodes into the network. Moreover, because of MANET distributed architecture and moving topology, a traditional centralized monitoring method is no longer feasible in MANETs.

II. ROUTING IN A MANETs

Routing in a MANET is intrinsically different from traditional routing found on infrastructured networks. Routing in a MANET depends on many factors including topology, selection of routers, initiation of request, and specific underlying characteristic that could serve as a heuristic in finding the path quickly and efficiently. The low resource availability in these networks demands efficient utilization and hence the motivation for optimal routing in ad hoc networks. Also, the highly dynamic nature of these networks imposes severe restrictions on routing protocols. of routing control information among the nodes. .

Proactive and Reactive Routing Protocols Adhoc routing protocols can be broadly classified as being Proactive (or table-driven) or Reactive (on-demand). Proactive protocols mandates that nodes in a MANET should keep track of routes to all possible destinations so that when a packet needs to be forwarded, the route is already known and can be immediately used. On the other hand, reactive protocols employ lazy approach whereby nodes only discover routes to destinations on demand, a node does not need a route to a destination until that destination is to be the sink of data packets sent by the node. Proactive protocols have the advantage that a node experiences minimal delay whenever a route is needed as a route is immediately selected from the routing table. However, proactive protocols may not always be appropriate as they continuously use a substantial fraction of the network capacity to maintain the routing information . To cope up with this shortcoming, reactive protocols adopt the inverse approach by finding a route to a destination only when needed. Reactive protocols often consume much less bandwidth than proactive protocols, but the delay to determine a route can be significantly high and they will typically experience a long delay for discovering a route to a destination prior to the actual communicate.

III. BACKGROUND

A.IDS in MANETs

As discussed, due to the limitations of most MANET direction-finding protocols, nodes in MANETs assume that other nodes always work together with each other to transmit data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To speak this problem, IDS should be added to enhance the security level of MANETs. If MANET can identify the attackers as soon as they enter the network, we will be able to completely reject the potential harms caused by compromised nodes at the first time. IDSs generally act as the second layer in MANETs, and they are a great balance to existing proactive approaches. In this section, we mainly discuss three existing approaches, namely, Watchdog [6], TWOACK [4].

1.A) Watchdog: Marti *et al.* [6] proposed a scheme named Watchdog that goal to develop the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is contain of two portions namely, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. It is in charge for identifying malicious node misbehaviors in the network. Watchdog identifies malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node eavesdrops that its next node fails to forward the packet within a certain period of time, it raises its failure counter. Whenever a node's failure counter beats a predefined threshold, the Watchdog node says it is misbehaving. In this case, the Pathrater work together with the routing protocols to avoid the reported nodes in future transmission.

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

The Watchdog scheme be unsuccessful to identify malicious misbehaviors with the presence of the following: 1) limited transmission power; 2) receiver collisions; 3) ambiguous collisions; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

2.A) TWOACK: With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new methods to solve these problems. TWOACK proposed by Liu *et al.* [5] is one of the most main methodologies among them. In TWOACK scheme, Each node is required to send back an acknowledgment packet to the node that is two hops left from it. The dissimilar to many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Targeting to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK identifies misbehaving links by acknowledging every data packet transmitted over every three sequential nodes along the path from the source to the destination. Upon recovery 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 essential to work on routing protocols such as Dynamic Source Routing (DSR) [2].

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems in Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Because of the limited battery power nature of MANET, such redundant transmission process can easily degrade the life period of the entire network.

3.A AACK: ACK is an end-to-end acknowledgment scheme is shown in Fig. 1. In Fig. 1, the source node S sends out Packet1 without any overhead except 2 b of flag representing the packet type. All the intermediate nodes only forward this packet. When the destination node D receives Packet1, it is mandatory to send back an ACK acknowledgment packet to the source node S along the reverse order of the same path. Within a predefined time period, if the source node S obtains this ACK acknowledgment packet, then the packet transmission from node S to node D is successful.

4.A EACCK: The EAACK scheme was extended with the introduction of digital signature to prevent the attacker from forging acknowledgement packets. EAACK is consisted of three major parts, namely: Acknowledge (ACK), Secure-Acknowledge (S-ACK) and Misbehavior Report Authentication (MRA). In order to distinguish different packet types in different schemes, they included a two-bit packet header in EAACK. According to the Internet draft of DSR , there are six bits reserved in DSR header. In EAACK, two of the six bits were used to flag different type of packets. In the proposed scheme it was assumed that the link between each node in the network is bi-directional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its receiver.

i.ACK ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In ACK mode, node S first sends out an ACK data packet ad1 P to the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node D successfully receives ad1 P, node D is required to send back an ACK acknowledgement packet ak1 P along the same route but in a reverse order. Within a predefined time period, if node S receives ak1 P, 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.

ii.S-ACK: S-ACK scheme is an improved version of TWOACK scheme proposed by Liu et al.The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. In S-ACK mode, the three consecutive nodes (i.e. F1, F2 and F3) work in a group to detect misbehaving

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

nodes in the network. Node F1 first sends out S-ACK data packet to node F2. Then node F2 forwards this packet to node F3. When node F3 receives, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgement packet to node F2. Node F2 forwards back to node F1. If node F1 does not receive this acknowledgement packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S. 1 s adP 1 s adP 1 s akP 1 s akP. Nevertheless, unlike TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report.

iii).MRA:

The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. False misbehavior report can be generated by malicious attackers to falsely report that 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 is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate MRA mode, the source node first searches its local knowledge ase and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes 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 compare if the reported packet was received. If it is already received, then it is safe to conclude 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.

iv)DSA/RSA:EACCK has three parts namely, ACK,S-ACK,MRA are acknowledgement based detection schemes. They all relay on acknowledgement packets to detect misbehaviors in the network. Thus it is extremely important to ensure that all acknowledgement packets in EACCK 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,EACCK 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.

IV. PROBLEM DEFINITION

DSR performs multiple route discovery and no route repair methods in DSR. So DSR has more end-to-end delay, it increases the throughput of the network DSR based on source routing mechanism, if any link failure occurs in the network ,DSR send a unicast packet to the source giving the information about the broken link but source may change dynamically. DSR has more routing overhead, less frequent route discovery and E2E delay.DSR Increases the network overhead. It requires of pre distributed keys. The DSA algorithm has the limiting factor that only the

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

owner of the private key can create the digital signature hence it can be used to verify who created a message and anyone knowing the public key can verify the signature provided they are confident of the identity of the owner of the public key. With DSA, the entropy, secrecy, and uniqueness of the random signature value k is critical. Using the same value twice (even while keeping k secret),or using a predictable value, or leaking even a few bits of k in each of several signatures, is enough to break DSA. Every RSA initialization process requires the random selection of two very large primes. In RSA over DSA, citing that RSA could be used for encryption and digital signature applications, while DSA was strictly for digital signature application, the length of the plaintext that can be encrypted is limited to the size of n. In fact, the real length is even smaller than n because of the overhead introduced by the algorithms. As a result, the predominate approach is to generate a random secret key and encrypt that key with the RSA keys. The message is then encrypted using a symmetric cipher with the generated secret key

V. PROPOSED SYSTEM

The AODV packets carry only the destination address. AODV has potentially less routing overheads than other protocol and AODV route replies only carry the destination IP address and the sequence number. The advantage of AODV is that it is adaptable to highly dynamic networks. AODV broadcast the Route error message to all its neighbors. Route maintained in routing table and AODV allows frequent route discovery and route discovery based on shortest and freshest.

DSR performs multiple route discovery and no route repair methods in DSR. So DSR has more end-to-end delay, it increases the throughput of the network. AODV has less routing overhead and end-to-end (E2E) delay which has high throughput. Number of sending and receiving packets increases in AODV due to less E2E delay. AODV acquires better performance than the DSR routing Protocol. Since, the Time taken for transmitting via AODV is less than the DSR. Also, the throughput is also compared between both the protocols. In that scenario also AODV outperforms than the DSR Routing. Instead of DSA/RSA Elliptic Curve Cryptography (ECC) is to provide a more secured transmission. Eliptic curve cryptosystems are based on the Discrete Logarithm Problem. Even if it uses shorter keysize, ECC provides same security level as RSA. The security of ECC is mainly due to difficulty of solving the elliptic curve discrete logarithm problem (ECDLP).So the attacks over ECC try to solve ECDLP problem. The main advantage of ECC is its high security level with smaller key size.

VI. PERFORMANCE EVALUATION

A. Simulation Configurations

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 10.24. In NS 2.34, the default configuration specifies 25 nodes in a flat space with a size of 670 × 670 m. The maximum hops allowed in this configuration setting are four. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. For each scheme, we ran every network situation three times and calculated the average performance.

To measure and compare the performances of our proposed scheme, we carry on to adopt the Packet delivery ratio performance metrics [13].

1)Packet delivery ratio (PDR): It defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. It has been calculated for both DSR and AODV protocol .Because of less end-to-end delay, Aodv has much more ratio of sending and receiving packets than DSR.ECC provides more secure packets delivery throughAODV.

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

2)*Latency Evaluation:* It has been calculated for both aodv and dsr protocol.DSR protocol has more end-to-end delay and routing overhead. if simulation time increases, performance reflects as more delay in transmission process. Due to less routing overhead in ECC,ECC provides less end-to-end delay.

3) *Throughput Evaluation*: DSR performs multiple route discovery and no route repair methods in DSR. So DSR has more end-to-end delay, it increases the throughput of the network. AODV has less routing overhead and end-to-end(E2E) delay which has high throughput. Number of sending and receiving packets increases in AODV due to less E2E delay. Due to less of malicious nodes in ECC,ECC provides much more ratio of sending and receiving by using small key size.

VII. CONCLUSION AND FUTURE WORK

Time taken for transmitting via AODV is less than the DSR. Also, the throughput is also AODV outperforms than the DSR Routing.In DSA, Using the same value twice (even while keeping k secret),or using a predictable value, or leaking even a few bits of k in each of several signatures, is enough to break DSA. Every RSA initialization process requires the random selection of two very large primes. In RSA over DSA, citing that RSA could be used for encryption and digital signature applications, while DSA was strictly for digital signature application, the length of the plaintext that can be encrypted is limited to the size of n. In fact, the real length is even smaller than n because of the overhead introduced by the algorithms. As a result, the predominate approach is to generate a random secret key and encrypt that key with the RSA keys. The message is then encrypted using a symmetric cipher with the generated secret key. With these limitations the EAACK approach needs to be further optimized for the digital signature schemes.In future,Instead of DSA/RSA Elliptic Curve Cryptography(ECC) is to provide a more secured transmission. Eliptic curve cryptosystems are based on the Discrete Logarithm Problem.Even if it uses shorter keysize,ECC provides same security level as RSA.The security of ECC is mainly due to difficulty of solving the elliptic curve discrete logarithm problem (ECDLP).So the attacks over ECC try to solve ECDLP problem.The main advantage of ECC is its high security level with smaller key size.

REFERENCES

[1] Elhadi M.Shakshuki, Nan Kang,Tarek R.Sheltami K.(2013)"EACCK-A Secure Intrusion Detection System for MANETs" IEEE Trans.Industrial Electronics,
vol. 60,no. 3,pp. 1089-1098.

[2] Suneth Namal,Konstantinos Georgantas and Andrei Gurtov(2013) "Lightweight authentication and key management on 802.11 with eliptic curve cryptography",
IEEE Wireless communication and Networking conf., vol. 48, no. 5, pp 1830-1835.

[3] N.Kang,E.Shashuki and T.Sheltami,(2011)"Detecting forged Ackowledgements in MANETs"in proc IEEE Int.conf.AINA,Biopolis, vol. 15, no. 5, pp 484-497

[4] N.Naser and Y.Chen(2007) "Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Adhoc Network"in proc.IEEE int.conf.commun.,Glasgow,Scotland, vol .147 no.18 pp .384-387.

[5] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan,(2007) "An Acknowledgment based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–55

[6] N. Kang, E. Shakshuki, and T. Sheltami,(2010) "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France,vol. 8,no .8, pp. 216–222.