IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver.VIII (Feb. 2014), PP 32-36
www.iosrjournals.org

Hybrid Cryptography Algorithms for Enhanced Adaptive Acknowledgment Secure in MANET

Ramya K[1], Beaulah David[2], Shaheen H[3]
PG Scholar Nehru Institute of Technology Coimbatore-641105 Tamilnadu
Assistant Professor Nehru Institute of Technology Coimbatore-641105 Tamilnadu
Assistant Professor Nehru Institute of Engineering and Technology Coimbatore-641105 Tamilnadu

Abstract: *The mobile adhoc network is a group of mobile nodes without having the fixed infrastructure. Due to the infrastructure less network and distributed nature, make mobile adhoc network susceptible to malicious attackers. So, we use an intrusion detection system called Enhanced Adaptive ACKnowledgement (EAACK) especially for mobile adhoc networks. Based on the digital signature algorithm (DSA) and RSA the EAACK is designed. To enhance the strength of the security in the mobile adhoc networks, we introduce an innovative approach called Hybrid Security Protocol that provides integrity, confidentiality and authentication. This Hybrid Security Protocol consists of Cryptography based on Elliptic curve, Dual-RSA algorithm and Message Digest MD5. Encryption is achieved by using Elliptic Curve Cryptography, Dual-RSA algorithm for authentication and MD-5 for integrity. By using a combination of both symmetric and asymmetric cryptographic techniques, we achieve better security with integrity.*

Key Terms:*Digital Signature, Enhanced Adaptive Acknowledgment (EAACK), Mobile Ad hoc Network (MANET), Elliptic Curve Cryptography, Dual-RSA, Message Digest-5.*

I. Introduction

Usually mobile adhoc network consists of a collection of mobile nodes, where each node in the MANET acts as both transmitter and receiver. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. Due to nodes lack of physical protection, malicious attackers can simply detain and compromise nodes to achieve attacks. It is used in military applications, commercial applications that demonstrate the safety of the information is an important problem. To address this problem an intrusion detection system is used to improve the security in MANET. Existing Intrusion detection systems like watchdog listen to it next hop's transmission. With a particular period of time the node fails to forward the packet the watchdog node increases the counter value. If counter value exceeds the threshold, it reports the node is misbehaving. After that the TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. But the problem is for every data packet transmission the acknowledgement process is required that produces the network overhead.

EAACK is the novel approach decides the problems of Preceding approaches by the combination of Digital signature and the RSA concepts. EAACK is an acknowledgement based IDS. The three parts of EAACK are ACK, S-ACK and MRA are acknowledgement based detection schemes. It is significant to ensure all acknowledgement packets in EAACK are authentic and untainted. Otherwise, if the attackers are easily to forge acknowledgement packets, all of the three schemes will be vulnerable. So, that we use a digital signature in the EAACK scheme. The digital signature scheme, all acknowledgement packets is digitally signed before they are sent out, and verified until they are accepted. But in the digital signature it requires additional resources in MANETs. To tackle this concern, we applied both DSA and RSA digital signature scheme.

To enhance the security in the mobile adhoc networks, we introduce an innovative approach called Hybrid Security Protocol, because it is desired to communicate data with high security. The Hybrid Security Protocol is a combination of both symmetric and asymmetric cryptographic techniques. The symmetric key cryptographic techniques include Elliptic Curve Cryptography, and Message digests MD5. It is used to achieve both the Confidentiality and Integrity. The asymmetric Key cryptographic technique includes, Dual RSA. It is used for the authentication. This new security protocol has been premeditated for better security using a combination of both symmetric and asymmetric cryptographic techniques.

II. Related Work

David B. Johnson et al. suggested dynamic source routing protocol for the mobile adhoc networks. Because in the mobile adhoc networks the mobile hosts are randomly moved [1]. Due to the limited range of transmission one mobile node needs other mobile node to forward the data packets. The dynamic source routing protocol adjusts quickly to routing changes when host movement is frequent. But it requires little overhead

during the frequent host movement. Source routing is one of the routing techniques in that the sender of the packet determines the entire sequence of nodes to forward the data packets. The sender clearly lists the route in the packet header, finding the each forwarding hop by the address of the next node to transmit the packet to the destination. The source routing either uses static or dynamic source routes. The dynamic source routing protocol employs no periodic routing advertisement messages, thereby decreasing network bandwidth overhead, predominantly during periods when little or no important host movement is taking place compared to the conventional routing protocols. In addition to that, the battery power is also reduced in the mobile adhoc networks.

Kejun Liu et al. proposed an Acknowledgment-based Approach to detect the routing misbehavior of the mobile adhoc networks [2]. TWOACK is necessary to work on routing protocols such as Dynamic Source Routing (DSR). The main idea of the two acknowledgement method is when a node forwards a data packet, effectively through the next hop, the next-hop link of the destination node will send back a special two-hop acknowledgment called 2ACK to specify that the data packet has been received successfully. TWOACK identifying the misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. The advantage of the two acknowledgement scheme is it has the flexibility to control the network overhead.

Jin-Shyan Lee et al. proposed a command filtering framework to allow or reject the human-issued commands so that unwanted executions are never performed [3]. In this concept the instead of using the client-server architecture the peer-to-peer (P2P) communication between mobile robots is used. A command filter is used to avoid the improper control actions from being carried out as the robot receives the human commands. Through the wireless network the human operator sends command requests to the mobile robot. Through the distributed P2P communication the command filter acquires the system status and makes decision to accept or reject the commands so as to meet the specifications. The function of the command filter is to interact with the human operator and the mobile robot so that the closest human-in the- loop system satisfies the requirements and guarantees that undesirable executions never occur. Through the P2P communication, there is an increase in scalability, robustness, and fault tolerance, resilience to attack and better support and management in distributed cooperative environments.

AnimeshPatcha et al. proposed Collaborative Security Architecture for detecting the Black hole attack in the mobile adhoc networks [4]. In this method, if the node forwards the data packet to the watchdog node identifies whether the next node also forwards the data packet. If the next node does not forwards the data packet the watchdog node makes it is misbehavior node. Every packet that is overheard by the watchdog is compared with the packet in the buffer to observe if there is a match. A match verifies that if the packet has been successfully delivered or not. After the timeout period the data packet has remained in the buffer, and then a failure tally for the node responsible for forwarding the packet is incremented. If this tally exceeds a predetermined threshold, then the node is termed as malicious and the network is informed accordingly. But the watchdog, sometimes wrongly reports other nodes are misbehaving.

SevilŞen et al.A proposed Intrusion detection system for the mobile adhoc networks [5]. In the absence of a fixed infrastructure to provide communications, mobile adhoc network is an attractive technology for some applications like environmental monitoring, conferencing, military applications. Due to the temporary infrastructure of the mobile adhoc network security is a significant concern. So, in order to overcome this problem the intrusion detection system is used. In the intrusion detection system there are three main components called collection of data, data detection, and response. The data collection component is used to collect and pre-process the data tasks. Transfer the data, data storage and sending data to the detection module. In the detection componentdata is analyzed to detect intrusion attempts and indications of detecting intrusions are sent to the response component.

M. Tamer Refaei et al. suggested a model to detect the node misbehavior in the mobile adhoc networks [6]. Based on the Sequential Probability Ratio Test we develop a model to describe how nodes can differentiate between routes that include misbehaving nodes and routes that do not. For the detection of the misbehaving nodes in the infected routes a centralized and a localized approach is used. The centralized approach assumes overall knowledge of all infected routes in the network. The localized approach assumes only local knowledge of such routes. We evaluate the ability of each to detect misbehaving nodes and the false positives and false negatives each incurs. The sequential Probability Ratio Test is easy to distinguish between infected and clean routes. Thus the localized approach performs much better, achieving high exposure and low false positives.

AnandPatwardhan et al. suggested secure routing and the intrusion detection system in the adhoc networks [7]. We present a proof-of-concept implementation of a secure routing protocol based on AODV over IPv6 for the Intrusion Detection and Response system for ad-hoc networks. The secure adhoc on-demand routing protocol has two concepts. One is Secure binding between IP version 6 (IPv6) addresses and the RSA key generated by the nodes themselves, and independent of any trusted security service. Another one is Signed evidence created by the originator of the message and signature verification by the destination, without any form

of designation of trust. Normally in the AODV protocol the route discovery mechanism is used to discover the route to the destination. An AODV message contains the RSA public key of the source node and that it is digitally signed to ensure the node's authentication and message integrity. Every intermediate node authenticates the verifies the source node.

Yih-Chun Hu et al. proposed a new secure on-demand ad hoc network routing protocol, called Ariadne to prevent attackers or the compromised nodes [8]. Ad hoc networks necessitate no fixed network infrastructure such as base stations or access points, and can be rapidly and economically set up as needed. By using one of the three schemes the Ariadne can authenticate the routing messages. A shared secret key is used between the all pairs of nodes. A shared secret key between communicating nodes shared with digital signatures. The pair wise shared key evades the necessity for harmonization, but at the cost of higher key setup overhead. Ariadne also necessitate that each node has an authentic component of the Route Discovery chain of every node initiating Route Discoveries. These keys can be set up in the similar method as a public key.

III. Intrusion Detection Approaches

1.1 Enhanced Adaptive Acknowledgment Scheme

EAACK is based on both DSA and RSA algorithm. The three main parts of the EAACK scheme are ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). EAACK is an acknowledgement based IDS. This scheme uses the digital signature method to prevent the attacker from forging acknowledgment packets. Before the acknowledgement packets sent out EAACK requires the whole acknowledgement packets are digitally signed and verified by its receiver until they are accepted. EACK shows that high malicious behavior rates without decreasing the network performances.

1.2 Acknowledgement

ACK is principally end-to-end acknowledgement scheme. It performs as a part of the hybrid scheme in EAACK, intend to reduce network overhead when no network misbehavior is detected. In the ACK mode, the node S sends the ACK data packet P_{ad1} to the destination node D. After that, all the intermediate nodes between the source and destination are cooperative and node D successfully receives P_{ad1} Packet it requires to send the ACK packet P_{ak1} back to the node S with same route but in reverse order. If in a particular time the node S receives the packet the data transmission is successful. Otherwise, node S will change to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes.

3.3 Secure Acknowledgement

In the S-ACK scheme to detect the misbehaving nodes every three successive nodes work in a group. In the three successive nodes the S-ACK acknowledgment packet is sent by the third node to the first node. The S-ACK scheme is able to detect the misbehaving nodes in the presence of receiver collision and low transmission power. In the S-ACK scheme the three consecutive nodes F1, F2, and F3 work as a group to identify the misbehavior of the nodes. At the first node F1 sends the S-ACK packet P_{sad1} to node F2. Then the node F2 forwards to node F3. After the node F3 receives the P_{sad1} Packet it is responsible to send back acknowledgement packet S-ACK P_{sak1} packets to node F2. Node F2 P_{sak1} to F1. Within a predefined threshold time the node N1 does not receive the acknowledgement packet the node F2 and F3 are malicious nodes. This can be reported by F1 node and inform to the source node.

3.4 Misbehavior Report Authentication

Actually, in the watchdog it fails to identify the misbehaving nodes due to the presence of a false misbehavior report. Because of this false report information the watchdog reports normal nodes as malicious nodes. To overcome this problem, the MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. For this the source node seeks its local knowledge base and identifies the other route to the destination node. If there is no route to destination by using the DSR routing request to find the alternate route. When the MRA packet is received by the destination node, it compares with using the local knowledge base whether the reported packet was received or not. If already received it make a decision, it is a false misbehavior report.

3.5 Digital Signatures

The three parts of EAACK are ACK, S-ACK and MRA are acknowledgement based detection systems. To detect the misbehaviors in the network, the three schemes rely on acknowledgment packets. All acknowledgement packets in the EAACK are authentic and untainted. Otherwise the attackers forge the acknowledgement packets; all the three schemes are susceptible. So, we include digital signature in EAACK to ensure the integrity of the intrusion detection system. It requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. But it requires additional resources due to

the digital signature in mobile adhoc networks. To overcome this we DSA and RSA digital signature schemes are used in MANETs.

3.6 Hybrid Security Protocol Architecture

Security is an important concern to communicate with others. To provide high security for information on controlled networks different types of cryptographic algorithms are used. These cryptographic algorithms are required to provide data security and user's authenticity. By utilizing a combination of both symmetric and asymmetric cryptographic techniques, the new security protocol has been designed for better security. This Hybrid security protocol provides three cryptographic primitives such as integrity, confidentiality and authentication. With the help of Elliptic Curve Cryptography technique, Dual-RSA algorithm and Message Digest MD5, these three primitives can be achieved. Public –key cryptography is also known as asymmetric cryptography, which requires two separate keys one of which is secret (or private) and one of which is public. In the symmetric key cryptography same key is used for both encryption and decryption. Elliptic Curve Cryptography and MD5 are Symmetric Key Cryptographic Techniques are used to achieve both the Confidentiality and Integrity. Dual RSA is Asymmetric Key Cryptography is used to achieve Authentication.

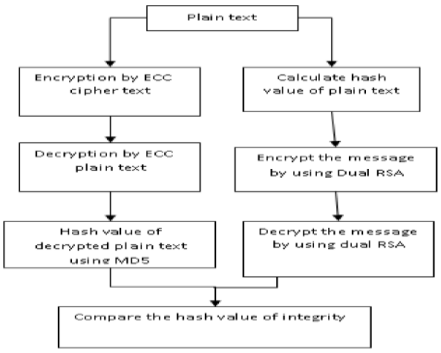

Figure 1 Architecture Diagram

By using the Elliptic Curve Cryptography the given plain text can be encrypted and the resulting cipher text can be communicated to the destination through any secured channel. At the same time by using the MD5 the hash value is calculated for the same plain text which already has been changed into the cipher text by ECC.With Dual RSA this Hash value has been encrypted and the encrypted message of this Hash value also sent to the destination. From the encrypted messages, the intruders may try to hack the original information. The intruder may get both the encrypted messages in plain text and the hash value and he will try to decrypt these messages to get original one. The attacker gets the hash value and it is not possible to extract the plain text from the cipher text, because, the hash value is encrypted with Dual RSA and the plain text is encrypted with ECC. Therefore, the message can be communicated to the destination with highly secured manner, by using the MD5 the new hash value is calculated for the received original messages with a decrypted hash message for its integrity. We make sure that either the original text being changed or not in the communication medium. This is the primary feature of this hybrid protocol.

IV. Exprimental Result

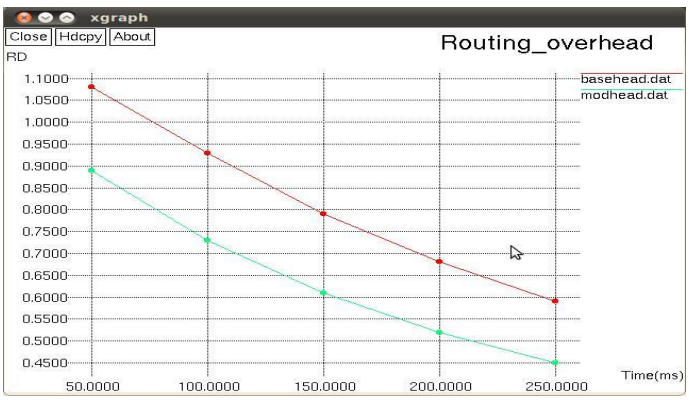

Figure 2.Routing Overhead graph

4.1 Routing overhead (RO)

RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].The graph of Routing Overhead is shown in following Fig.1in which time ranging from 50 to 250 milli seconds is taken along x–axis and Routing Overhead ranging from 32 to 44 $\times$ 10^{-3} is taken along y–axis. We observe that EAACK (DSA and RSA) and EAACK (MD5+dual RSA) scheme achieve the best performance, as the scheme to detect misbehaviors. This is largely due to its hybrid architecture, which significantly reduces network overhead. Although EAACK (MD5+ dual RSA) requires all acknowledgment process, it still manages to maintain lower network overhead in most cases.

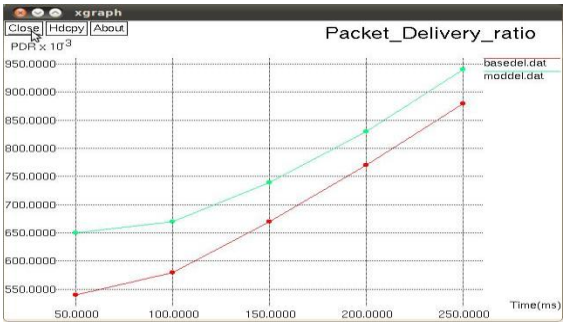

Figure 3. Packet Delivery Ratio Graph

4.2 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. The graph of Packet Delivery Ratio is shown in following Fig.2, in which timing ranging from 50 to 250 milli seconds is taken along x–axis and PDR ranging from 780 to 940*10^{-3} is taken along y–axis. We can infer, as the number of nodes increases, the packet delivery ratio also increases because there are more route choices for the packet transmission. Among the two response mechanisms, we also notice the packets delivery ratio of EAACK ((MD5+ dual RSA)) response is higher than those of other approach EAACK (RSA and DSA).

V. Conclusion

To provide security in the mobile adhoc networks we use a novel intrusion detection system called EAACK. Including digital signature in EAACK to prevent the attackers from initiating forged acknowledgment attacks. In the EAACK all acknowledgement packets are digitally signed before they sent out and verified until they are accepted. The packet delivery ratio is improved, but it consumes more resources. So, DSA and RSA schemes are used in the mobile adhoc networks. To enhance the security we use Hybrid Security protocol is used. It is a combination of both symmetric and asymmetric cryptographic techniques. The Hybrid Security protocol includes Elliptic Curve Cryptography technique, Dual-RSA algorithm, Message DigestMD5 are responsible for integrity, confidentiality and authentication. For future work a key management scheme is used that does not require any Trusted Third Party (TTP) for key management. In thekey management system, before joining the network both a new node and group leader authenticates each other.

References

[1] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

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

[3] 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.

[4] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in *Proc. Radio Wireless Conf.*, 2003, pp. 75–78.

[5] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[6] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[7] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in *Proc. 3rd Int. Conf. Pervasive Comput. Commun*, 2005, pp. 191–199.

[8] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2002, pp. 12–23.

[9] 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.

[10] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros- Mendez, "Energy harvesting from piezoelectric materials fully integrated in footwear," *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 813–819, Mar. 2010.