International Journal of Computer Applications (0975 - 8887)
Volume 123 - No.4, August 2015

UNIACK- Universal Adaptive Acknowledge Intrusion Detection System in Manets

Lohar Priyanka D.
Computer Engineering Department,
JSPM's BSIOTR,Wagholi, Pune, India

Lomte Archana C.
Computer Engineering Department,
JSPM's BSIOTR,Wagholi, Pune,India

ABSTRACT

MANET (Mobile Ad-Hoc Network) a unique network which provides communication between mobile nodes available outside or within the radio range. This unique feature migrated from wired network to wireless network and resulted in the security issues. So, there is need to secure the MANETs. As compared to other types of networks, MANETs are more vulnerable to different attacks such as black hole attack, gray hole attack, wormhole attack, etc. MANET decides a radio range within which node can move and can feasibly transmit the data. And if any of the nodes migrates from one radio range to another, it relays the messages to their neighbors. This means that two communicating nodes are notable to exchange messages if those nodes exceed the radio range. To avoid these types of attacks, different Intrusion Detection System (IDS) in MANETs are introduced to follow secure data transmission. In this paper, a secure IDS plays an important role and gives the system which improves the efficiency of EAACK (Enhanced Adaptive Acknowledge) and is compared with different IDS in MANETs using RSA, AES and ZRP algorithms. RSA algorithm is used for encryption and decryption of the message to securely transmit data using mathematical model. AES algorithm is combinely used with RSA. And ZRP (Zone Routing Protocol) divides network into small zones to decide the route with nearby nodes and ensure the authentic path in the mobile network.

Keywords

Hybrid Cryptography,Zone Routing Protocol,AES,RSA,IDS in Manets

1. INTRODUCTION

An autonomous nature of system Mobile Ad hoc Network (MANET) of mobile routers (and related hosts) connected by wireless links the union of which form an arbitrary graph [1]. The can freely move and organize themselves arbitrarily; which results in change and unpredictably of network?s wireless topology. Migration from wired network to wireless network in recent days played an important role resulting existence of infrastructure less setup. In ad hoc networks high degree of mobility is combined with wireless communication. And that enables it to deploy in extreme and volatile situations. MANETs have been proposed for use in many areas such as tactical operations, monitoring of any system and conferences and so on [4]. Nature of MANET is open, infrastructure less and dynamic topology provides the flexibility but introduces different security risks. So to avoid these risks, security measures must be taken to identify these risks and take appropriate actions. The system design can be based on risk prevention or risk avoidance. The nature of MANETs depends upon security issues to be taken under consideration are as follows: First, Ad hoc networks are followed by passive eaves dropping that is to masquerade till active interference of attackers [5]. Second, Deployment of security mechanisms are resulted due to lack of trusted third party and CA. Third, Due to limited power consumption and computation capabilities of mobile devices which make it more prone to Denial of Service (DoS) attacks and are incapable of execution of computationally heavy algorithms like public key algorithms [8]. Fourth, in MANETs, trusted node are compromised in large amount and launch attacks on networks, in another word; there is need to consider both insider attacks and outsider attacks in mobile ad hoc networks, in which insider attacks are more difficult to deal with. Finally, due to mobile nature of nodes in MANETs, there is need to reconfigure network frequently which creates more chances for attacks[5]. Ability to allow data communication between different parties and still maintain their mobility is one of the advantages of MANETs. Communication is carried out within the range of the transmitter. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own[7][9].

MANETS gives installation of Intrusion Detection System (IDS) in each and every node. Following are some of the basic IDS that are available are:

(1) Watchdog Scheme [10]
(2) Two Ack Scheme
(3) Adaptive Acknowledgment

These schemes are suffered with various disadvantages like receiver collision, limited power transmission problem, false misbehavior report, ambiguous collision, and partial dropping.First node sends packet to next node, third node is required to send back S-ACK packet to first node otherwise second and third nodes are malicious. Then MRA scheme checks that whether misbehavior report is authentic by checking that particular reported missing packet is received by receiver through some other route. If it happens, destination node then node which generate this report is marked as malicious. Otherwise false misbehavior report is trusted and destination node is marked as malicious [10]. Existing system of EAACK used Digital Signature is to digitally sign the packets both at the sender and receiver side to prevent the forging of packets. Thus

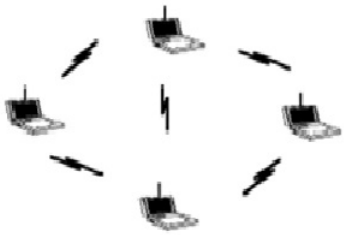

Fig. 1. Infrastructure less Network with mobile nodes

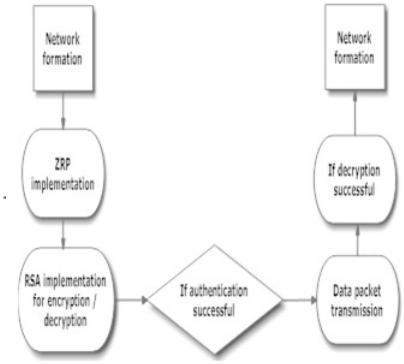

Fig. 2. Proposed system architecture.

there is need for implementing digital signature and both DSA and RSA are used. The safe exchange of packets is done through the existing system EAACK scheme which involves digital signature. In this work both Digital Signature Algorithm (DSA) and RSA algorithms are implemented. By comparing both algorithms, DSA produces less network overhead than RSA, as the signature size of DSA is smaller when compared to RSA. As the number of nodes increases the frequency of data transfer increases resulting in Routing Overhead (RO) of malicious nodes increases in RSA, than DSA. Hence more malicious nodes results in more acknowledgment of packets, thus increasing the usage of digital signature in network. As EAACK scheme depends on acknowledgement of packets, it is necessary to reduce the network overhead caused by digital signature. Our research work, focus on providing IDS for MANETS, which reduces network overhead and provides security to network. Proposed hybrid key cryptography technique reduces the network overhead. As the count of malicious nodes gets increased, network overhead also get increased.Advantage of different types of multiple ciphers used called as hybrid cryptosystem protocol. The main advantage of proposed cryptography protocol is using innovative techniques to conceal secret session key which is transferred among sender and receiver throughout unsecured channel.

2. RELATED WORK

Implementation of a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to other approaches, EAACK gives higher malicious behavior-detection rates in certain conditions while does not greatly affect the network performances. Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. As compared to Watchdog, TWOACK and AACK results in the cases of receiver collision, limited transmission power, and false misbehavior report retain positive performance [7]. Intrusion Detection Techniques for Node Cooperation in MANETs. Intermediate nodes might agree to forward the packets but actually drop or modify them because they are misbehaving. An intrusion detection system is run on each node independently to determine intrusions. Every decision made is based only on information collected at its own node, since there is no co-operation among nodes in the ad hoc network [1]. To evaluate the performance impact of security approach in SEAD without attackers, it is modified as the DSDV-SQ implementation in extensions to ns-2[3]. In this, increased the size of each routing update to represent the authentication hash value in each table entry. Each node is initially placed at a random location and pauses for a period of time called the pause time [3]. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which to forward the packet. The sender explicitly lists route in the packets header, identifying each forwarding hop by the address of the next node to which to transmit the packet on its way to the destination host. This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach [4].

3. PROPOSED SYSTEM

Proposed hybrid key cryptography technique reduces the network overhead. The main advantage of proposed cryptography protocol was using innovative channel. MANET provide mobility feature techniques to conceal secret session key which is transferred among sender and receiver throughout unsecured which deals with mobile nodes in the network. Formation of the network already existed network compatibility is the feature of this type of network. A feature which is to deal with this type of network, security is the main issue. To deal with the security issues the algorithms taken into consideration are ZRP, RSA and AES algorithms chosen as a benchmark algorithm. The hybrid cryptography techniques are Digital Signature Algorithm (RSA) and Advanced Encryption Standard (AES). Fig (b) shows the proposed architecture. Proposed architecture is designed considering following modules:

A) Network Formation
B) ZRP implementation
C) Implementation of RSA

D) Implementation of AES
E) Analysis

A. Network Formation
Preprocessing includes deploying values for one-hop transmissions.The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670 670 m. Both the physical layer and the 802.11MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000s. For each scheme, ran every network scenario three times and calculated the average performance. In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics:
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.
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].
Zone Routing Protocol
Zone Routing Protocol (ZRP) is a Hybrid protocol which combines the advantages of both proactive and reactive approaches. For route discovery reactive routing protocols involves long route request delays and inefficient flooding, while proactive routing protocols uses excess bandwidth to maintain routing information. It takes advantage of proactive discovery within a node?s local neighborhood, and using a reactive protocol for communication between these neighborhoods. In Ad-Hoc mobile network, it can be supposed that the most communication takes place between nodes closer to each other. Therefore, ZRP decreases the proactive scope to a zone centered on each node. In a limited zone, the routing information can be maintained easily and the amount of routing information that is never used is also minimized. Since all nodes proactively store local routing information, nodes farther away can be reached with reactive routing.
Implementation of RSA
It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. In this proposed system, RSA algorithm is used to securely transmit data from sender to receiver.
Implementation of AES
AES formats plaintext into 16 byte (128-bit) blocks, and treats each block as a 4x4 State array. It then performs four operations in each round. The arrays contains row and column information used in the operations, especially Mix Columns () and Shift rows (). This algorithm is mainly used to provide security for the secret information and also to reduce network overhead then the performance will be improved.
Analysis
Performance of the proposed scheme is analyzed and its security as well as energy and communication cost also analyzed. If there is any node act as adversaries then that node also analyzed for identifying which type of loss they will produced. Simulation results are identified and it is compared with the existing system in case of energy consumption, throughput, delay, efficiency in terms of security level are also analyzed and furthermore tested on real network. Analysis is done through the principle is to let every three consecutive nodes work in a group to detect misbehaving nodes

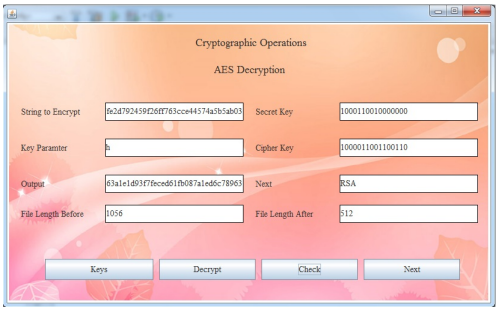

Fig. 3. Decrypted data upon applying AES Algo

called as Misbehavior Report Authentication based on EAACK.

4. ALGORITHM

As this proposed system based on Hybrid Cryptography, RSA and AES Algorithms are supposed to combine and make more secure transfer of the data. ZRP Algorithm is supposed to use for routing the data on authenticated path.

RSA ALGORITHM
1. Input two prime numbers
2. Compute n = pq
3. Compute the totient
4. Choose e ¿ 1 coprime to 3120
5. Compute d by modular multiplicative inverse of e modulo: d

AES ALGORITHM
1. Initially use Add round key stage followed by 9 rounds of four stages and a tenth round of three stages.
2. 16 X 16 matrix of byte values called an s-box
3. Follow bitwise compliment of a for s-box(a) = a
4. Shift second row 1 byte to the left in a circular manner
5. Shift third row 2 bytes to the left in a circular manner
6. Mix Column transformation A-1 = A-1AS = S
7. 128 bits of state are bitwise XORed with the 128 bits of the round key.

5. RESULTS

Upon applying those algorithm considering both Existing system and Proposed system the performance is measured in considering encryption and decryption of message to be sent.

6. CONCLUSION

Hence by using Hybrid Cryptograpy new system is designed called UNIACK which overcomed problems faced in base paper that is EAACK and the new system is implemented using RSA and AES algorithms combined with gave high performance reduced traffic overhead and average end to end delay as MANETs has mobile

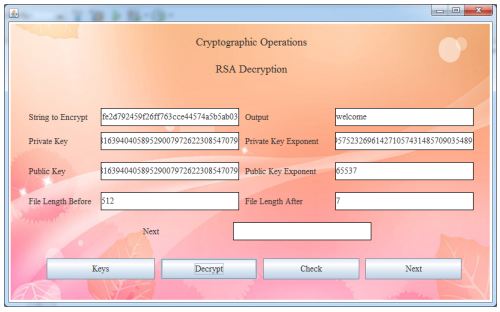

Fig. 4. Decrypted data upon applying RSA Algo on the same message.

Fig. 5. Decrypted data upon applying SHA Algo on the same message.

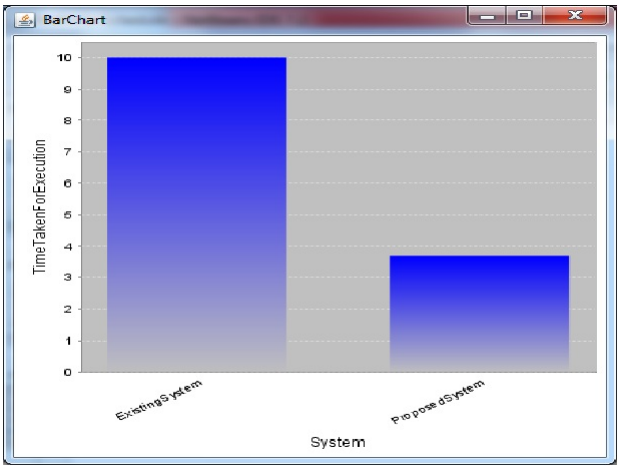

Fig. 6. Comparing performance of Existing System and Proposed System.

nodes within the radio range. New approach named as Uniack Intrusion Detection System is assumed as a benchmark approach in dealing with problems faced in EAACK system upon partial fulfillment of this new approach and by implementing on real network. respect to this result,it is found DSA as a more desirable digital signature scheme in MANETs. The reason is that data transmission in MANETs consumes the most battery power. Although the DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable.In future this system, UNIACK can be enhanced by using more poweful algorithms to increase in performance and efficiency.

7. REFERENCES

[1] Tiranuch Anantvalee and Jie Wu in Wireless/Mobile Network Security Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp.170 ? 196 c 2006 Springer ? ?A Survey on Intrusion Detection in Mobile Ad Hoc Networks.

[2] Vehbi C. Gungor, Member, IEEE, and Gerhard P. Hancke, Senior Member, IEEE IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 56, NO. 10, OCTOBER 2009 ?Industrial wireless sensor networks: Challenges, design principles, and technical approach.

[3] Yih-Chun Hu a, David B. Johnson b, Adrian Perriga at Ad Hoc Networks 1 (2003) 175192 SEAD secure efficient distance vector routing for mobile wireless ad hoc networks.

[4] David B. Johnson and David A. Maltz book Mobile Computing, edited by Tomasz Imielinski and Hank Korth Kluwer Academic Publishers, 1996. Dynamic Source Routing in ad hoc wireless networks.

[5] Lidong Zhou Zygmunt J. Haas in IEEE network, special issue on network security, November/December, 1999 Securing ad-hoc networks?.

[6] R.L. Rivest, A. Shamir, and L. Adleman National Science Foundation grant MCS76-14294, and the Office of Naval Research grant number N00014-67-A-0204-0063. ”A method for obtaining digital signatures and public- key cryptosystems”.

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

[8] Safdar Ali Soomro , Sajjad Ahmed Soomro , Abdul Ghafoor Memon in Journal of Information and Communication Technology Vol. 4, No. 2, (Fall 2010) 01-10 ?Denial of Service Attacks in Wireless Ad hoc Networks.

[9] Khaldoun Al Agha, Senior Member, IEEE, Marc-Henry Bertin, Tuan Dang, Member, IEEE, Alexandre Guitton,Member, IEEE, Pascale Minet, Thierry Val, and Jean-Baptiste Viollet IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 56, NO. 10, OCTOBER 2009 ”Which Wireless Technology for Industrial Wireless Sensor Networks? The Development of OCARI Technology”.

[10] K.P.Manikandan and Dr.R.Satyaprasad ”Analysis and Diminution of Security Attacks on Mobile Ad hoc Network ” JCA Special Issue on Mobile Ad-hoc Networks MANETs” 2010.