ISSN:0975-9646

An Enhanced Intrusion Detection System for MANETS using Hybrid Key Cryptography

B.Suruthi[1] Mr.N.V.Rajeesh kumar.M.Tech[2]

[1]*Student,M.E.computer Science and Engg,*
Sathyabama University,Chennai.
[2]*Faculty Computer Science and Engg,*
Sathyabama University, Chennai.

***Abstract:-*Wireless networks are mostly preferred nowadays, because of its mobility and scalable characteristics. Of all the available wireless networks, Mobile Ad-hoc NETworks (MANET) is the most important and typical application. MANET has the changing topology and it does not have the fixed network infrastructure. Each node act both as the transmitter and receiver and node configuration is done on its own. Nodes communicate among themselves either directly or with the help of neighbors. The open medium allows MANET vulnerable to attacks. In existing system Enhanced Adaptive Acknowledgment(EAACK) method is imposed, in this digital signature method is used which cause network overhead. Thus proposed system specifies the Hybrid Cryptography technique is used to reduce network overhead.**

***Keywords:*Mobile** *Ad-hoc NETwork (MANET), Digital Signature, Enhanced Adaptive ACKnowledgment(EAACK).*

I.INTRODUCTION

MANETS are wireless networks, and decentralised and no fixed topology. Each node in network act both as transmitter and receiver. Nodes communicate with each other either directly or indirectly (with the help of their neighbors).Hence this is possible by single hop network and Multi-hop networks. In Single-hop network, all the nodes within the same radio range communicate with each other. In Multi-hop network, nodes depend on neighbors to transmit if destination node is out of their radio range. MANET is highly vulnerable to attacks because, node configuration and maintenance are done on its own. Then Enhanced Adaptive ACKnowledgement scheme is used to overcome the disadvantage of false misbehaviour report. MANET are mostly preferred for military, areas that include natural disaster, medical emergency.

In next section related work is explained, then existing system which explains Enhanced Adaptive ACKnowledgement in detail, and proposed system explains about Hybrid Cryptography Technique.

II.RELATED WORK

1.EAACK-A Secure Intrusion Detection System for MANETS, Elhadi M.Shakshuki, Nan Kang, Tarek R.Sheltami, explains various IDS in MANET and its disadvantages, EAACK its support in solving false misbheaviour report problem.

2. A Survey on Intrusion Detection in Mobile Ad-hoc Networks in wireless/mobile security, T.Anantvalee J.Wu, provides survey of various Intrusion Detection implementation in mobile ad-hoc networks.

3.Ad-hoc mobile wireless networks routing protocol-A review, G.Jayakumar G.Gopinath, explains different routing protocols like reactive and proactive protocols and its importance in MANET.

4.Detecting misbehaving nodes in MANETS, N.Kang M.Shakshuki T.Sheltami, clarifies the methods in identifying malicious nodes caused by attacks, and some ways to prevent the network from intruders.

5.Detecting Forged acknowledgments in MANETS, N.Kang E.Shakshuki, specifies the security is based on acknowledgement packets, how to safeguard those packets from attacks.

6.Enhanced intrusion detection system for discovering malicious nodes in mobile ad-hoc network, N.Nasser Y.Chen, provides an improved technique Enhanced Adaptive Acknowledgement for detecting malicious nodes in network.

7.A method of obtaining digital signatures and public-key cryptosystems, R.Rivest A.Shamir L.Adleman, significant ways of enveloping packets with digital signature and public-key cryptosystems.

8.Industrial wireless sensor networks: challenges, principles and technical approach, V.C.Gungor G.Hanke, provides the various applications of wireless networks in industries.

III.EXISTING SYSTEM

In MANETS Intrusion Detection System are installed in each and every node. Some of the basic IDS that are available are,

1. Watchdog scheme
2. Twoack scheme
3. Adaptive Acknowledgment.

These schemes are suffered with various disadvantages like receiver collision, limited power transmission problem, false misbehaviour report, ambiguous collision, and partial dropping.

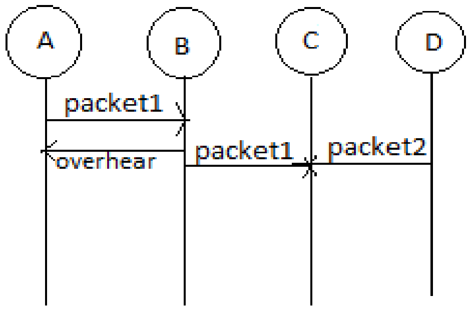

Fig 1: Receiver Collision occurs at receiver C because both B and D send packets at same time.

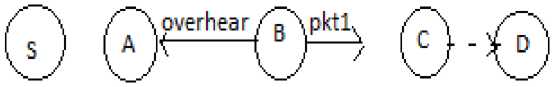

Fig 2: Limited transmission power problem leads C unable to receive pkt1 from B but it can be overheard by A.

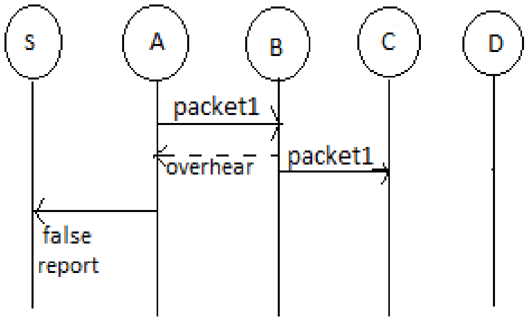

Fig 3: False misbehaviour report-send by node A to source S that node B is malicious though B forwards packet1 to node C.

Later, a new technique called Enhanced Adaptive Acknowledgment is introduced. It solves all the three above issues. This technique depends on acknowledged packets. So it also includes Digital Signatures to prevent the attackers from attacking the packets.

EAACK consist of 3 parts namely:

1. ACK
2. Secure ACK(S-ACK)
3. Misbehaviour Report Authentication (MRA).
4. Digital Signature.

In ACK scheme, source node should get the acknowledgment packet within the predefined time period, it implies that destination node receives the packet and no malicious node exists in the route, otherwise send secure ACK packet.

The intention of introducing S-ACK mode is to find malicious node by forming every three nodes into one group. 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 is to check whether misbehaviour report is authentic by checking that reported missing packet is received by receiver via some other route. If destination node already receives this packet then node which generates this report is marked as malicious. Otherwise false misbehaviour report is trusted and destination node is marked as malicious.

Digital Signature is used to digitally sign the packets both at the sender and receiver side to prevent the forging of packets. Thus required resources need to be incorporated for implementing digital signature and both DSA and RSA can be used.

IV. Problem Definition

The existing system has EAACK scheme which involves digital signature for safer exchange of packets. This is implemented by both Digital Signature Algorithm (DSA) and RSA algorithms. Comparing both algorithms, DSA produces lesser network overhead than RSA, because the signature size of DSA is smaller when compare to RSA. Routing Overhead (RO) will be more if the number of malicious nodes increases in RSA, than DSA.Because more malicious nodes involves more acknowledgment packets, thus increasing the usage of digital signature in network.

Thus EAACK scheme depends on acknowledged packets. So, its necessary to reduce the network overhead caused by digital signature.

Our research work, focus on providing an IDS for MANETS, which reduces network overhead and provides security to network.

V.Proposed System

In this paper, we propose a hybrid key cryptography technique that reduce the network overhead. Network overhead increases when number of malicious node in network increases, because the count of acknowledged packet increases. Thus to reduce network overhead Hybrid key cryptography technique is used.

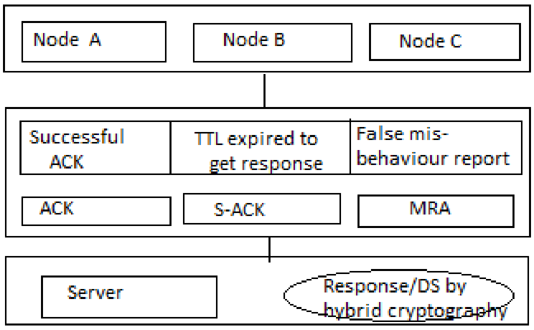
Node A
Node B
Node C
Successful ACK
TTL expired to get response
False mis-behaviour report
ACK
S-ACK
MRA
Server
Response/DS by hybrid cryptography

Fig.4 System Architecture

The proposed system uses RSA and AES (Advanced Encryption Standard).

First, it is required to find the route between source and destination this is possible by ZRP (Zone Routing Protocol).It is a hybrid protocol. This protocol divides the entire network into zones. It makes use of any of reactive or proactive protocols within and between the zones. Size of the zone is given by parameter r. Intra-zone routing is provided mostly by proactive protocol, thereby reduces delay to communicate to nodes within network. Inter-zone routing uses reactive protocol, this avoids the need to keep proactive fresh state of the entire network. ZRP also defines a technique called Bordercast Resolution Protocol (BRP) to control the traffic between the zones. If a node has no route to its destination by proactive inter-zone routing, BRP is used to spread the reactive route request.

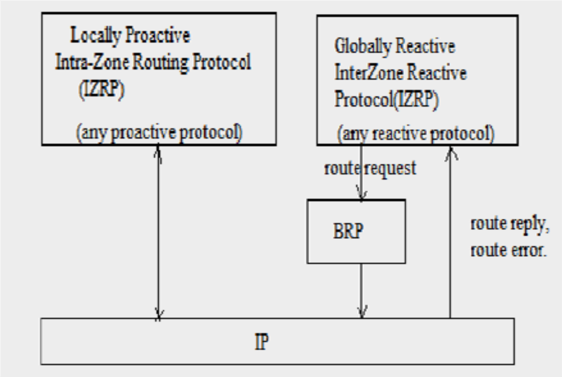

Fig.5. Components of ZRP

VI.Conclusion And Future Work

The newly proposed scheme called EAACK, and it provides better performances comparing to all other existing approaches. The EAACK scheme implements digital signature which causes network overhead which can be further reduced by hybrid key cryptography. This cryptography technique uses RSA, AES for providing security and Zone Routing Protocol (ZRP) to find the route between source and destination.

The future work :

To allow the execution of EAACK scheme in real time environment to obtain accurate results for testing.

References

[1].Elhadi M. Shakshuki, Senior member, IEEE, Nan Kang, and Tarek R.Sheltami, IEEE; EAACK – A Secure Intrusion Detection System for MANETS; IEEE Transactions on Industrial Electronics, vol.60,No.3, March 2013.

[2].R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Commun.ACM, vol. 21,No.2,pp. 120-126, Feb 1983.

[3]. William Stallings, Cryptography and Network Security, Fourth Edition, June 3, 2010.

[4]. G. Jayakumar, G.Gopinath, Ad hoc mobile wireless networks routing protocol-A review, vol. 3, No. 8, pp. 574-582, 2007.

[5]. T.Anantvalee and J.Wu, A Survey on Intrusion Detection in Mobile Adhoc Networks, NewYork: Springer 2008.

[6]. Minimized Routing Protocol in Ad-hoc Network with Quality Maintenance Based on Genetic Algorithm: A Survey, Upasna, Jyoti chauhan, Manisha, IJSRP, vol. 3, Issue 1, January 2013.

[7]. R.H.Akbani, S.Patel and D.C.Jinwala, DOS attacks in mobile adhoc networks, A Survey in proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012,pp.535-541.

[8]. A Secure data transmission in MANETS using Hybrid Scheme, Sowmya Thomas, Syam Gopi, IJERT,Vol. 2, Issue 8,August 2013.

[9]. Dr.E. Ramaraj, S. karthikeyan, M.Hemalatha, A Design of Security Protocol Using Hybrid Encryption Technique(AES-Rijndael and RSA) International Journal of the Computer, the Internet and Management, Vol.17, No.1,(January-April 2009)pp 78-86.

[10]. Y.Hu.D.Johnson, and A.Perrig, and D.Johnson, ARIADNE: A Secure on-demand routing protocol for ad -hoc networks, pp. 3-13.

[11]. Hybrid cryptography by the implementation of RSA and AES, Palaniswamy. V, Jeneba Mary, International Journal of Current Research, Vol. 33, Issue 4, pp. 241-244,april 2011.

[12]. N.Kang, E.Shakshuki and T.Sheltami, Detecting forged acknowledgements in MANETS, in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, March 2011, pp.488-494.

[13]. N.Kang, E.Shakshuki, and Sheltami, Detecting misbehaving nodes in MANETS, in Proc. 12th Int. Conf. IIWAS, Nov.2010, pp.216-222.

[14]. K. Liu, J. Deng, P. K.Varshney, and K.Balakrishnan, An acknowledgment-based approach for the detection of routing misbehaviour in MANETS, IEEE Trans. Mobile Computing, vol. 6,no.5, pp. 536-550.

[15]. N.Nasser and Y.Chen, Enhanced Intrusion Detection systems for discovering malicious nodes in mobile ad hoc networks, in Proc. IEEE Int. Conf. Commun, Glasgow, Scotland, June 2007, pp.1154-1159.