ISSN: 2321-7782 (Online)
Volume 3, Issue 1, January 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

An Intrusion Detection System for MANET using Hybrid Cryptography

Deepti A. Chaudhari[1]
PG Student,
Department of Computer Engineering,
JSPM's RSCOE, Tathawade
Pune – India

Prof. S. B. Javheri[2]
Associate Professor,
Department of Computer Engineering,
JSPM's RSCOE, Tathawade.
Pune – India

Abstract: ***Over the decade, security has become a most important issue in Mobile Adhoc Network compared to other networks, MANETs are more weak to the various types of attacks. In this case the detection should be focused as another part before an attacker can harm the structure of the system. A new intrusion detection system named Enhanced Adaptive ACKnowledgement (EAACK) is specially intended for MANET. By the acceptance of MRA scheme, EAACK is capable of detecting malicious nodes regardless of the existence of false misbehavior report. For this concern an Enhanced Adaptive Acknowledgment (EAACK) has been developed with Hybrid cryptography (DES and RSA). By adopting this technique, it further reduces the network overhead which is caused by digital signature in previous system. To increase the security level of packet, prime number generation of RSA is done by Genetic Algorithm. The results will show positive performances in opposition to EAACK with DSA and EAACK with Hybrid Cryptography.***

Keywords: ***Enhanced Adaptive ACKnowledgement (EAACK)(AACK), Malicious nodes , MANET, Secure Intrusion Detection Systems (SIDS).***

I. INTRODUCTION

The mobility and scalability has been provided by wireless networks, which made it popular among people from using wired network. Wireless networks can be classified into two type, they are infrastructure and adhoc network[1]. In infrastructure-based networks, communication takes place only between the wireless nodes and access points, but not directly between the wireless nodes. Collisions may occur if the access point is not coordinated. They cannot be used for disaster relief in cases where no infrastructure is available. On the other hand Adhoc network has no need of any network infrastructure to work[6]. Each node can communicate directly with other nodes. Mobile Adhoc Network (MANET) consists of wireless mobile nodes that form a temporary network without the fixed infrastructure or central administration [3]. Here nodes can communicate directly to one another within their transmission range. Nodes those are outside the transmission range are communicated via intermediate nodes. For proper functioning of the network, cooperation between nodes is important. MANET is highly vulnerable to attacks because some of the unique characteristics of adhoc wireless networks, such as open infrastructure, dynamic network topology, lack of central administration and limited battery power of mobile nodes. In order to save its own battery resources a node may misbehave by agreeing to forward packets but fail to forward [7].

Both routing packets and data packets forwarding function would be affected in the presence of misbehaving nodes. The node misbehavior can be classified into 3 types. They are malfunctioning, selfish and malicious [8].

Malfunctioning: nodes suffer from hardware or network failures.

Selfish: nodes refuse to forward or drop data packet.

Malicious: nodes use their resource and aims to weaken other nodes or whole network, by trying to participate in all established routes thereby forcing other nodes to use a malicious route which is under their control.

The rest of the paper is organized as follows. In Section 2, related work survey. Section 3 gives Implementation Details. Section 4 shows results. Section 5 conclusion and future work.

II. LITERATURE SURVEY

Elhadi M. Shakshuki et al.[1] presents their work on EAACK—A Secure Intrusion-Detection System for MANET they focuses on the self-configuring ability of nodes in MANET and they made it popular among vital mission applications like military use or emergency recovery.

The authors propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to modern approaches, EAACK demonstrates privileged malicious-behaviour-detection rates in definite situation while it does not greatly affect the network performances. The demonstrated results show positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehaviour report.

Rajeshkumar. G and K. R. Valluvan[2] presents the paper on comparative study of SIDS for detecting malicious nodes and gives an overview of IDs architecture for enhancing security level of MANETs based on security attributes and various algorithms namely RSA and DSA.

Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami[3] Detecting Forged Acknowledgments in MANETs presents the paper with the research work and introduce a Digital Signature algorithm(DSA) into EAACK scheme and investigate the performance of DSA in MANET.

K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan[4] presents paper as acknowledgment-based approach for the detection of routing misbehaviour in MANETs, This paper introduced TWOACK scheme which aims to solves the problem of receiver collision and limited transmission power of Watchdog. TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from source to destination. But the acknowledgment process required in every packet transmission proces added a considerable amount of unwanted network overhead.

Adnan Nadeem et al.(2013) [5] in their work on “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks” concentrates on mobile ad hoc networks (MANETs) that have emerged as a major next generation wireless networking technology. However, MANETs are vulnerable to various attacks at all layers, including in particular the network layer, because the design of most MANET routing protocols assumes that there is no malicious intruder node in the network.

III. IMPLEMENTATION DETAILS

3.1 System Design

The proposed system’s approach of EAACK is designed to deal with three of six weaknesses of watchdog scheme, particularly, false misbehavior, limited transmission power, and receiver collision.

The EAACK system consist following steps

- ACK
- Secure Acknowledgment (S-ACK)
- Misbehaviour Report Authentication (MRA)
- Hybrid Cryptography for packet Transmission

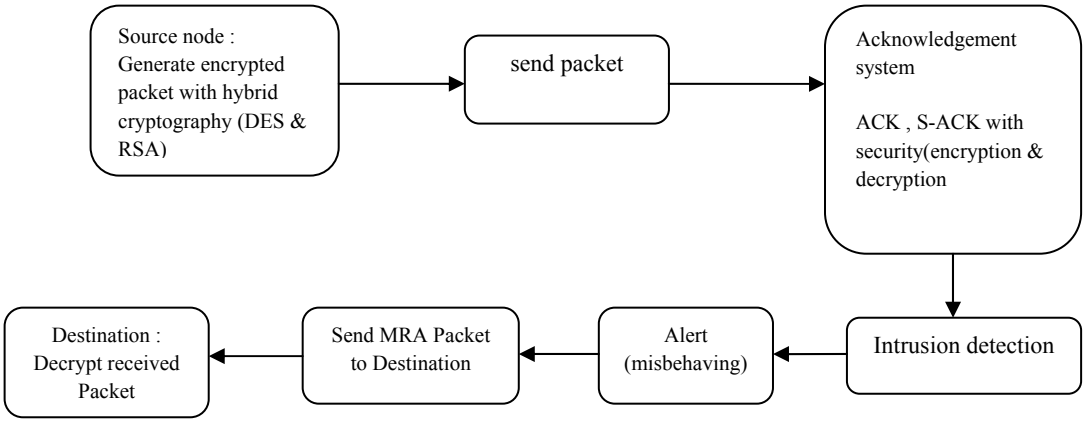

Fig. 3.1 System architecture diagram

3.1.1 ACK

Basically ACK is an end – to – end acknowledgment scheme .It is a part of EAACK scheme. The aim is to reduce the network overhead when no network misbehavior is detected. The basic flow is if source node S sends an ACK data packet P_{ad1} to destination Node D, and if all the intermediate nodes between S to destination node D are cooperative and successfully receives the P_{ad1}, then for node D it is essential to send back ACK acknowledgment packet P_{ack1} from the same route but in reverse order. If the P_{ack1} packet is received to node S in the predefined time period, then the packet transmission is successful from source node S to destination node D. Otherwise it switch to S-ACK mode and send out S-ACK data packet to detect misbehaving node in the route.

3.1.2 Secure acknowledgment (S-ACK)

In the S-ACK, the principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment 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.

3.1.3 Misbehaviour report acknowledgment (MRA)

This MRA scheme is designed to resolve the weakness of watchdog where it fails to detect the misbehaving node with the presence of false misbehavior report. This false misbehavior report can be generated by the attackers by reporting falsely for the innocent nodes as malicious.

The goal of MRA scheme is to authenticate whether the destination node has received the reported missing packet from a different route.

In the MRA mode source node searches for a alternate route to the destination node. If there is no other route is exists, the source node starts a DSR routing request to find another route. By adopting the alternate route for the destination node then it can avoid the misbehavior reporter node. When the destination node receives the MRA packet it searches it's knowledge base and compares to that the reported packet was received or not, if it is already received then it conclude that this is a false misbehaviour report and whoever send it, is marked as malicious. Otherwise the false misbehavior report is trusted and accepted.

3.1.4 Hybrid cryptography for Packet Transmission

Here DES and RSA are used for data encryption and decryption. The prime numbers for RSA are generated by the Genetic Algorithm, because of it, increases the security level. DES is symmetric key algorithm and RSA is asymmetric key algorithm. Asymmetric key algorithm requires private key and public key.

3.1.4.1 Key Generation

RSA has a public key and private key. Public key is known to every one and is used to encrypting messages. The messages which are encrypted using public key can only be decrypted using the private key. The steps for RSA algorithm are:

1. Choose two distinct prime numbers x and y.
2. For security purposes, the integer's x and y chosen uniformly at random and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
3. Compute m = xy.
   - m is used as the modulus for both the public and private keys
4. Compute the totient or $\Phi = (x-1)(y-1)$
5. Randomly choose an odd integer ep such that, $ep < \Phi$ and such that ep and Φ are relatively prime (gcd (ep, k) = 1)
   - ep is released as the public key exponent.
6. By using the extended Euclidian algorithm the decryption key dk has been generated. The formula of generating dk is $dk = ep^{-1} \bmod \Phi$.
   - Now public key is the pair of (ep, k) and private key dk.

3.1.4.2 Encryption

1. Encrypt data by DES algorithm, DES key encrypt by RSA
2. To encrypt the message using RSA encryption, sender must have receivers public key pair (ep, k)
3. The message to be send must be encrypted using this pair (ep, k).
4. To encrypt it , source simply computes the number 'A' where $A_i = msg_i^{ep} \bmod k$
5. Source sends the cipher text A to destination.

3.1.4.3 Decryption

1. To decrypt the cipher text A destination required to use it's own private key dk and the modules k.
2. The decryption formula is $msg_i = A_i^{dk} \bmod k$.
3. Which gives back the decrypted message msg.

3.2 Genetic Algorithm for Prime number generation

Algorithm f(l.k)

(1) Pass = 0;

(2) Randomly taken an odd integer p from within 10^l to 10^{l+1} ;

(3) Randomly taken k distinct integers from within 2 to n − 2 ; a1, a2 ,⋯ ⋅, ak;

(4) For i = 1 To k Loop

(5) Call subroutine Miller(n, a_i);

(6) If pass = 0 Then Goto (8)

(7) End Loop

(8)If Pass = 1; then we believe that p may be a prime number, otherwise, p must be a composite number, end.

Subroutine Miller (n, a_i)

(1) Calculate b = $a_i^{\ m}$ mod p;

(2) B = ±1 then Pass =1 and GoTo(8);

(3) Pass =0;

(4) For j = 1 To t −1 Loop;

(5) b = b^2 mod n;

(6) If b = −1 Then Pass =1 and Goto (8);

(7) End Loop

(8) End

IV. Result

The graphical representation of the system shows that Packet Delivery Ratio much better than previous system and Routing Overhead is reduced of EAACK system by adopting hybrid cryptography approach than the use of digital signature algorithm.

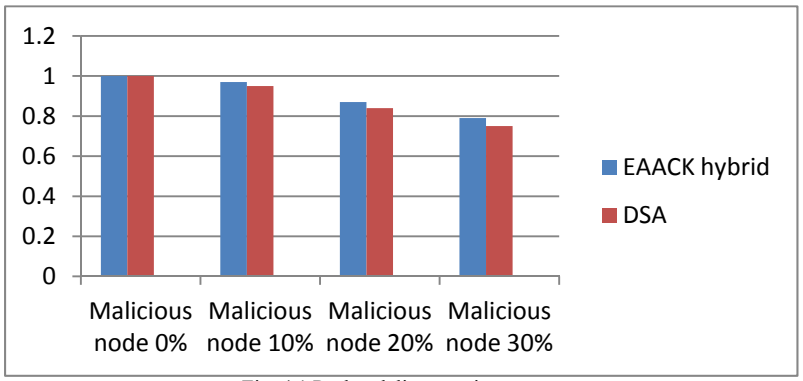

Fig. 4.1 Packet delivery ratio

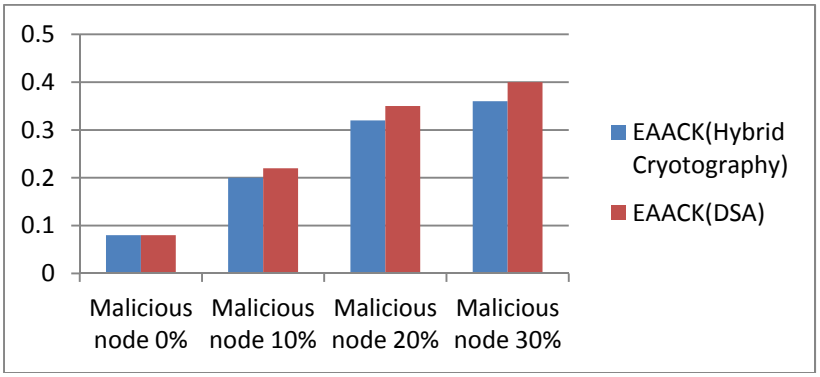

Fig. 4.2 Routing overhead

V. Conclusion and Future Scope

The proposed system goal is to find the optimal solution for using digital signature in MANET which causes a network overhead, depend on parameters are Packet Delivery Ratio(PDR), Routing Overhead. Hybrid cryptography is used to increase security level of data packet and also reduces the network overhead. In this technique the DES and RSA algorithm are used, also Genetic Algorithm is used for large prime number generation is used in key generation of RSA. The future scope is to examine the possibilities of Key Exchange mechanism to eliminate the requirement of predistributed keys.

References

1. Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami "EAACK –A Secure Intrusion-Detection System for MANETs" IEEE Transactions VOL.60,NO.3 MARCH 2013
2. U. Sharmila Begam, Dr. G. Murugaboopathi "A Recent Secure Intrusion Detection System for MANETs," International Journal of Emerging Technology and Advanced Engineering, Volume 3, Special Issue 1, January 2013
3. R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.
4. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.
5. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.
6. Rajeshkumar. G and K R Valluvan:" A Comparative Study of Secure Intrusion-Detection Systems for Discovering Malicious Nodes on MANET" International Journal of Computer Applications 67(18):1-5, April 2013.
7. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.
8. Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami "Detecting Misbehaving nodes in MANETs" iiWAS2010 Proceedings
9. 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.
10. Zhang Qing, Hu Zhihua, "The large prime numbers generation of RSA algorithm based on genetic algorithm," 2011 International Conference on intelligence Science and Information Engineering IEEE

