Rashmi K. Mahajan *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 12, December- 2014, pg. 97-102 **ISSN: 2321-8363**

EAACK, SECURE IDS FOR MANET BY USING CRYPTOGRAPHIC ECDSA ALGORITHM

Rashmi K. Mahajan[1], Prof. S. M. Patil[2]

[1] *Department of Electronics Engineering, Datta Meghe College of Engineering, Mumbai University, Airoli, Navi Mumbai 400708, Maharashtra, India*

[2] *Department of Electronics Engineering, Datta Meghe College of Engineering, Mumbai University, Airoli, Navi Mumbai 400708, Maharashtra, India*

Abstract

Providing security against the intruder is a challenging task in MANET due to unfixed topology, and lack of centralized control. Therefore it is crucial to develop suitable intrusion detection scheme (IDS) to protect MANET from malicious attackers. Most of the current Intrusion Detection Systems (IDSs) for MANETS rely on the Watchdog technique. To prevent the adversaries from forging the acknowledgement packets and to solve the issues regarding receiver collision, limited transmission power and false misbehavior problem of watchdog scheme a new Intrusion-detection system named modified Enhanced Adaptive ACKnowledgment (EAACK) using Elliptical curve cryptographic Algorithm (ECDSA) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher Malicious Behavior Detection rates in certain circumstances while does not greatly affect the network performances.

Keywords: Enhanced Adaptive ACKnowledgment (EAACK), Mobile Adhoc NETwork (MANET), Elliptic Curve Digital Signature Algorithm (ECDSA)

1. Introduction

In the recent years Mobile Ad-hoc Network (MANET) is emerging as a very popular technology in the wireless network due to its dynamic topology and its infrastructure less architecture as well as reduced cost with improved technology, Given this description, we find some limiting characteristics that make the Ad-Hoc wireless networks, very vulnerable to intruders and attacks that can damage the integrity of the network. Providing security against the intruder is a challenging task in MANET. Therefore it is crucial to develop suitable intrusion detection scheme (IDS) to protect MANET from malicious attackers. [1] The purpose of this project is to provide security along with identification of false misbehaving. Elliptic Curve Cryptography (ECC) algorithm is used to provide security to the data that is sent between the nodes.

2. Background

In this section, we primarily describe existing IDS approaches, namely, Watchdog [2], TWOACK [3], and adaptive ACKnowledgment (AACK) [4] and Enhanced Adaptive ACKnowledgment (EAACK) [6] And MANET's Security constraint with the use of Digital signature

A. Existing IDS for MANET

2.1 ***Watchdog*** – It aims to improve the throughput of network with the presence of malicious nodes. [2] Watchdog fails to detect malicious misbehaviors with the presence of 1) ambiguous collision;

2) receiver collision; 3) limited transmission power; 4) false misbehaving report; 5) collusion and 6) partial dropping.

2.2 ***TWOACK-*** Used to resolve receiver collision and limited transmission power of watchdog. TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. [3] TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) [5].

2.3 ***AACK-*** It is a combination of TWOACK [4] and end-to-end ACKnowledgement (ACK) scheme. It reduce network overhead.

2.4 ***EAACK-*** Used to detect misbehavior in the network. It is a combination of ACK, Secure ACK (SACK) and Misbehavior Report Authentication (MRA). [6]
ACK- It is a end-to-end acknowledgement scheme used to reduce network overhead when no network misbehaviour is detected.
S-ACK- It is a version of TWOACK. It is used to detect misbehaving node in presence of receiver collision and limited transmission power [6].
MRA- MRA is used to detect misbehaving node with presence of false misbehaviour report. False misbehaviour report can be generated by malicious attacker to falsely report innocent node as malicious.

B. Digital Signature

Digital signature may be a wide adopted approach to confirm the authentication, integrity, and nonrepudiation of MANETs. [7][8] the message is send to the hash function hash function is processed and then it sent to the message digest, the message digest is used to check the message whether the message is valid or not. And then it sent to the signature function, to verify the signature by applying public key or private key by using generalized as an information string. [9]

3. Problem Definition

TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehaviour attack. In this proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, limited transmission power, and receiver collision, false misbehaviour. We know the fact that more malicious nodes require more acknowledgment packets, thus increasing the ratio of digital signature in the whole network overhead. Many of the existing IDSs in MANETs adopt an acknowledgment based scheme, including EAACK. The functions of such detection scheme largely depend on the acknowledgment packets. Hence, it is guarantee that the acknowledgment packets are valid and authentic by using digital signature. Here, our goal is to propose an IDS specially designed for MANETs, which solves overhead caused by digital signature but also improve the security in system.

4. Proposed System Model

We propose a strong and light-weight enhanced Intrusion detection mechanism called EAACK protocol using ECDSA Algorithm which requires less cost, low power. EAACK is consists of three major parts called: ACK, S-ACK and MRA. ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehaviour is detected. According to this method, Refer Fig-1, if the receiver node does not send the ACK within predefined period, then ACK assumes malicious may present and switch to SACK part to detect them. In S-ACK part, 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. If malicious found, then MRA part suggests alternate path to the destination. Unlike the TWOACK scheme, where the source node immediately trusts the misbehaviour report, EAACK requires the source node to switch to MRA node and confirm this misbehaviour report. This is a vital step to detect false misbehaviour report in our proposed scheme.


```
While (True) Do
Read Data Packet;
Process it;
If  (node is destination node) Then
            Send SAck packet to previous node
 Else
     Start timer for PckID and wait for Sack packet to be  received
     If (SAck packet received in time)
          If  (PckID in SAck in list)
              Remove PckID and its timer from list
              Send SAck to previous node
          End
     Else
            Send PckID Data Packet to all neighbours and start timer and wait.
            Receive acknowledgement from neighbour
          If  (SAck packet is from next node)
            Remove PckID and its timer from list
            Send Sack to previous node
          Else
            Report next node as malicious node
End While
```

To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received, and then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Instead of RSA, Improved Cryptographic technique or Improved ECC is going to use. It ensures the secure communication of data packets in the network.

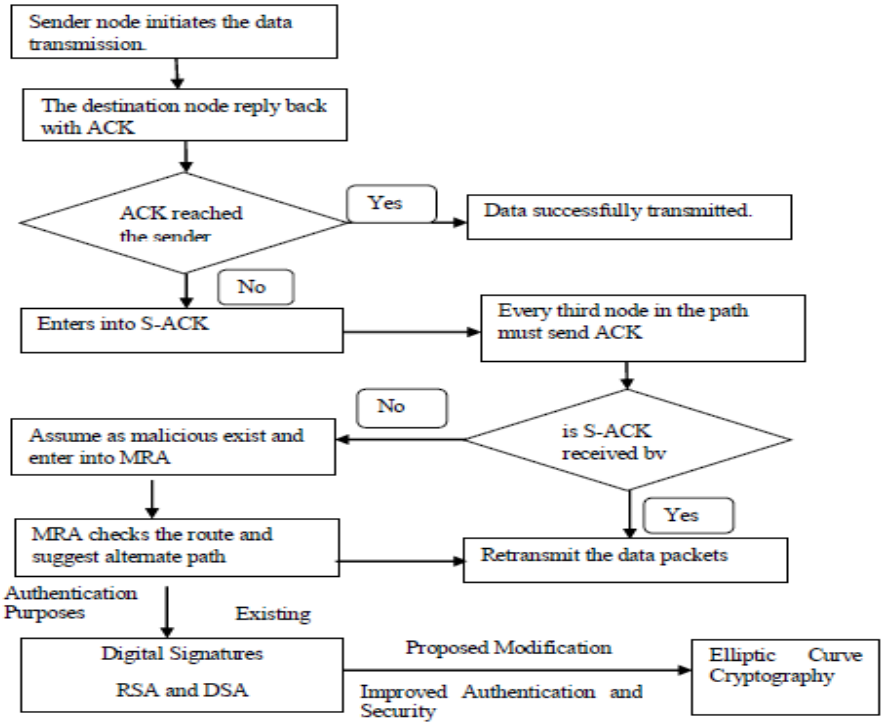

Fig-1 System Flow Diagram

5. Performance Evaluation

A. Methodology

Enhanced adaptive acknowledgement (EAACK) is an acknowledgement based intrusion detection system; in order to ensure all acknowledgement packets is authentic. They use digital signature algorithm (DSA) to sign the acknowledgement packets, digital signature algorithm (DSA) involves more routing overhead and energy consumption, Adopting hybrid cryptography techniques. To further reduce the network overhead caused by digital Signature without compromising its security. Here we proposes ECDSA instead of DSA to ensure that all acknowledgment packets in EAACK are authentic and untainted. ECDSA stands for "Elliptic Curve Digital Signature Algorithm", it's used to create a digital signature of data (a file for example) in order to allow you to verify its authenticity without compromising its security. [14]
ELLIPTICAL CURVE DISCRETE LOGARITHM PROBLEM (ECDLP) : The strength of the Elliptic Curve Cryptography lies in the Elliptic Curve Discrete Log Problem (ECDLP). The statement of ECDLP is as follows. Let E be an elliptic curve and P belongs to E be a point of order n. Given a point Q belongs to E with Q = mP, for a certain m belongs to {2, 3, ……, m – 2}. Find the m for which the above equation holds. When E and P are properly chosen, the ECDLP is thought to be infeasible. Note that m = 0, 1 and m – 1, Q takes the values ***O***, P and – P. One of the conditions is that the order of P i.e. n be large so that it is infeasible to check all the possibilities of m. [15][16]

B. Simulation Configurations

In this paper we concentrate on describing the simulation environment and the system of methods followed in a particular discipline as well as comparing performances through simulation result comparison with EAACK schemes. Our simulation is conducted in machine which has java with version JDK 1.6 and above. We used NetBeans IDE 7.4 version with minimum 256 MB RAM the coding has been done to simulate the concept which has been discussed the ECC algorithm which is providing high security while packet are send through the network from node to node.

C. Experimental Results

The Fig.2, 3 & 4 given is the results of our simulation showing EAACK packet mode.

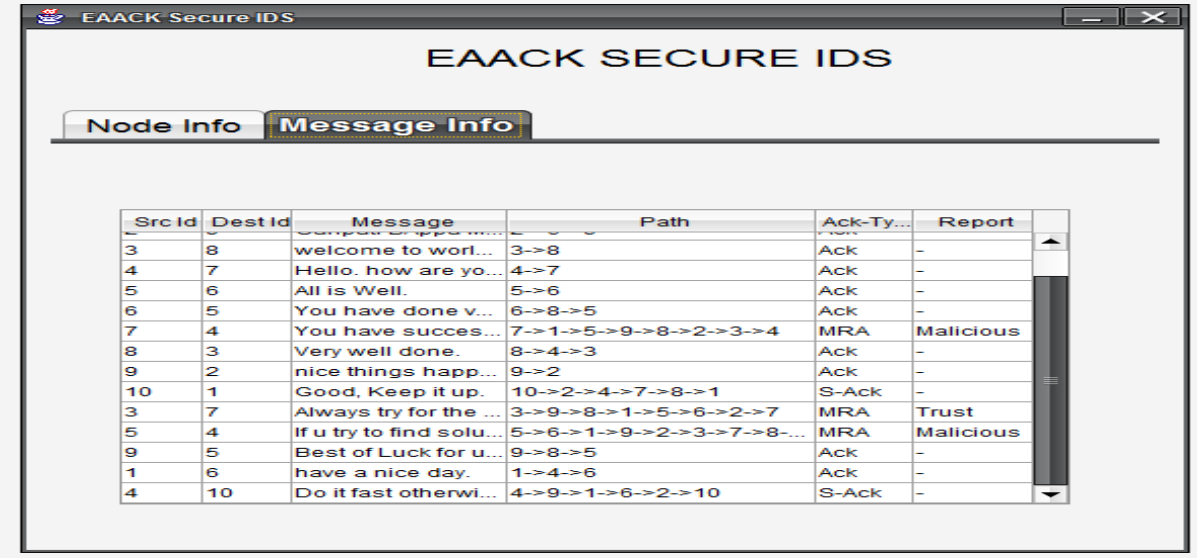

Fig.2 table showing communication details between so**u**rce and destination nodes in EAACK Secure ids

Encrypted message and Decrypted message is a function of key size and data size for both DSA/RSA and ECC. ECC key size is relatively smaller than DSA/RSA key size, thus encrypted message and Decrypted message in ECC is smaller as shown in Fig.5 & Fig.6. These results provide high quality in data delivery with high Security provided by ECC.

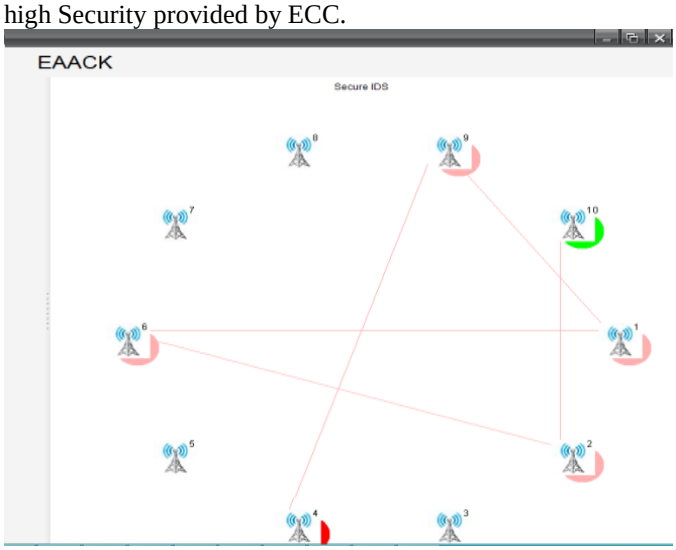

Fig.3 EAACK Secure ids n/w showing path tracing from Source node (4) to destination node (10) for message 15 from fig.9

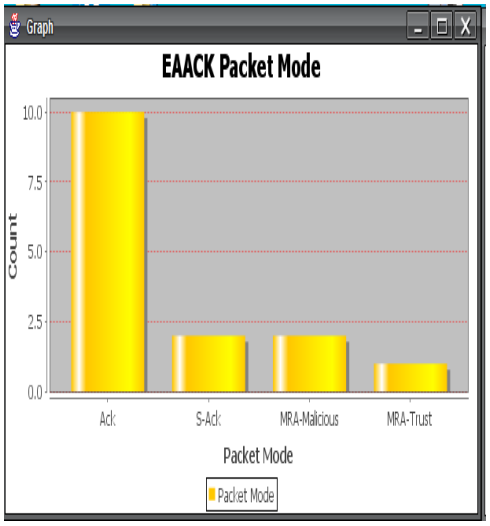

Fig.4 EAACK Secure ids Packet Mode

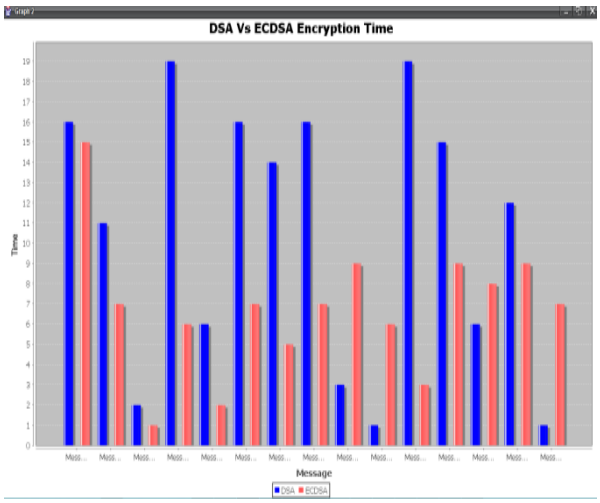

Fig.5 EAACK-DSA VS ECDSA Encryption Time

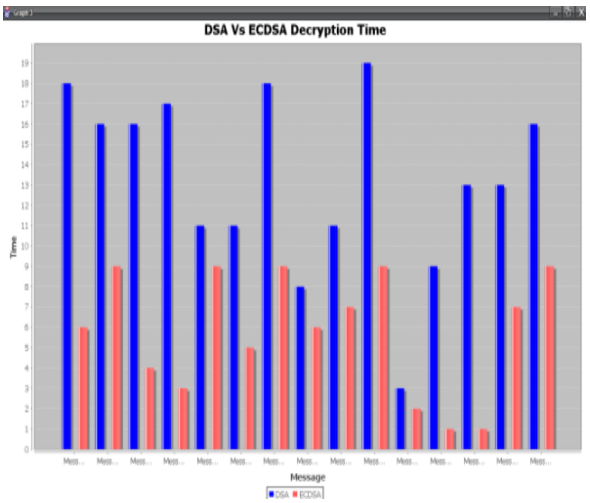

Fig.6 EAACK-DSA VS ECDSA Decryption Time

6. CONCLUSION AND FUTURE WORK

In this paper the main focus has been laid on comparative study of EAACK approach and its limitation with *EAACK protocol using ECC*. Here we have study the behaviour of EAACK technique. The algorithm is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of

false misbehaviour report and to authenticate whether the destination node has received the reported missing packet through a different route and to achieve this we have to focus on the comparative study of ACK, SACK & MRA scheme. To extend the deserves of our analysis work, we plan to Investigate the subsequent problems in our future research:
1) Potentialities of adopting hybrid cryptography techniques to additional cut back the network overhead caused by digital signature;
2) examine the chances of adopting a key exchange mechanism to eliminate the necessity of redistributed keys;
3) Testing the performance of EAACK in real network environment rather than software code simulation.

7. Acknowledgement

It is my immense pleasure to express my deep sense of gratitude and indebtedness to my highly respected and esteemed project guide Prof. S. M. Patil. His invaluable guidance, inspiration, constant encouragement, sincere critism and sympathetic attitude could make this paper possible.

8. References

1. Noman Mohammed, HadiOtrok, Lingyu Wang, MouradDebbabi and Prabir Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on DEPEDABLE and Secure Computing, 2011.
2. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.
3. 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.
4. T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes inMANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.
5. 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.
6. Ellade M.Shakshuki, Senior member, Nan Kang, and Tarek R.Sheltami, "EAACK-a secure intrusion detection system for MANETS" IEEE trans on industrial electronics, vol.60, No.3, March 2013.
7. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996, T-37.
8. M. Zapata and N. Asokan, "Securing *ad hoc* routing protocols," in *Proc ACM Workshop Wireless Secur.*, 2002, pp. 1–10.
9. Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).
10. K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2009.
11. 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.
12. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
13. V. Katiyar, K. Dutta, S. Gupta; "A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment." *International Journal of Computer Applications* 11(10):41– 46, December 2010.
14. Xu Huang; Shah, P.G.; Sharma, D.; , "Protecting from Attacking the Man-in- Middle in Wireless Sensor Networks with Elliptic Curve Cryptography Key Exchange," *Network and System Security (NSS), 2010 4th International Conference on* , vol., no., pp.588- 593, 1-3 Sept. 2010.
15. Yong Wang; Ramamurthy, B.; Xukai Zou; , "The Performance of Elliptic Curve Based Group Diffie-Hellman Protocols for Secure Group Communication over Ad Hoc Networks," *Communications, 2006. ICC '06. IEEE International Conference on* , vol.5, no., pp.2243-2248, June 2006.
16. A. Al-Maashri, M. Ould-Khaoua, Performance Analysis of MANET Routing Protocols in the Presence of Self-Similar Traffic, Proceedings of 31st IEEE Conference on Local Computer Networks, 14-16 Nov. 2006, pp. 801–807.

