CEAACK based Detector for Malicious Nodes

Meenakshiammal.R
AP/IT
PET Engineering College
Vallioor, Tirunelveli

Deivanayaki.N
AP/CSE
PET Engineering College
Vallioor, Tirunelveli

N.Shalini
AP/IT
PET Engineering College
Vallioor, Tirunelveli

ABSTRACT

MANET stands for Mobile Ad Hoc Network. The Ad Hoc network that is used for mobile communication is called MANET. The MANETS are used when the user is moving. Because MANET does not depends on fixed infrastructure. Wireless networks are used to connect with different networks in MANETs. Security is more critical in wireless communication when compared to the wired communication. So the security of the MANET must be optimized to secure information while transferring. The proposed system introduces a new intrusion-detection system named Competent Enhanced Adaptive Acknowledgment (CEAACK) for finding malicious nodes using RSA digital signature and EAACK specially designed for MANETs.

General Terms

Intrusion Detection System, Security, Wireless communication

Keywords

EAACK, RSA Digital Signature, MANET

1. INTRODUCTION

1.1 Network Security

Network administrator or System administrator is responsible for network security. [19] He implements the security policy; network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensure that employees have adequate access to the network and resources to work.

A network security system typically relies on layers of protection and components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network.

1.2 MANET

Mobile Ad hoc Network (MANET) is one of the most important and unique applications. In contrast with traditional network architecture, MANET does not require a fixed network infrastructure [10], every single node works as both a transmitter and a receiver. Nodes can be communicated directly with each other if they are within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion detection mechanisms to protect MANET from attacks. In this paper, we propose and implement a new intrusion-detection system named Competent Enhanced Adaptive Acknowledgment (CEAACK) specially designed for MANETs. Compared to contemporary approaches, CEAACK demonstrates higher malicious behavior detection rates in certain circumstances while does not greatly affect the network performances.

2. OBJECTIVE

The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is vital to develop efficient intrusion-detection mechanisms to protect MANET from attacks. In this paper, we propose and implement a new intrusion-detection system named Competent Enhanced Adaptive Acknowledgment (CEAACK) specially designed for MANETs. CEAACK is consisted of three major parts, namely, ACK, Secure ACK (S-ACK), and Misbehavior Report Authentication (MRA) [13] with digital signature. And the information is encrypted using AES Algorithm.

3. EXISTING SYSTEM

The researches had provided number of collaborative IDS systems namely

1. Watch dog
2. TWOACK
3. AACK
4. EAACK

Watchdog: By listening to its next hop's transmission watch dog [17] detects malicious behaviours. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving.

TWOACK: Misbehaving links are detected by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is indebted to generate a TWOACK [16] packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three consecutive nodes along the rest of the route.

AACK: It is a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). In the ACK scheme, the source node S sends out Packet 1. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet.

EAACK: It is used to detect the malicious nodes with the help of acknowledgement and MRA Report. Existing system doesn't use any key exchange mechanism to distribute keys. [13]

4. PROPOSED SYSTEM

A new intrusion detection system named Competent Enhanced Adaptive Acknowledgement (CEAACK) is specially designed for MANETs. This proposed system uses Diffie-Hellman key exchange for distributing secret key used for AES algorithm. The original information is encrypted by AES and is signed by sender and is forwarded to receiver. Receiver verifies sign & decrypts the packet to obtain the message. By the adoption of MRA scheme, CEAACK is capable of detecting malicious nodes despite the existence of false misbehavior report and compared it against other popular mechanisms in different scenarios through simulation. CEAACK demonstrates higher malicious behavior detection rates in certain circumstances while does not greatly affect the network performances.

5. SYSTEM ARCHITECTURE

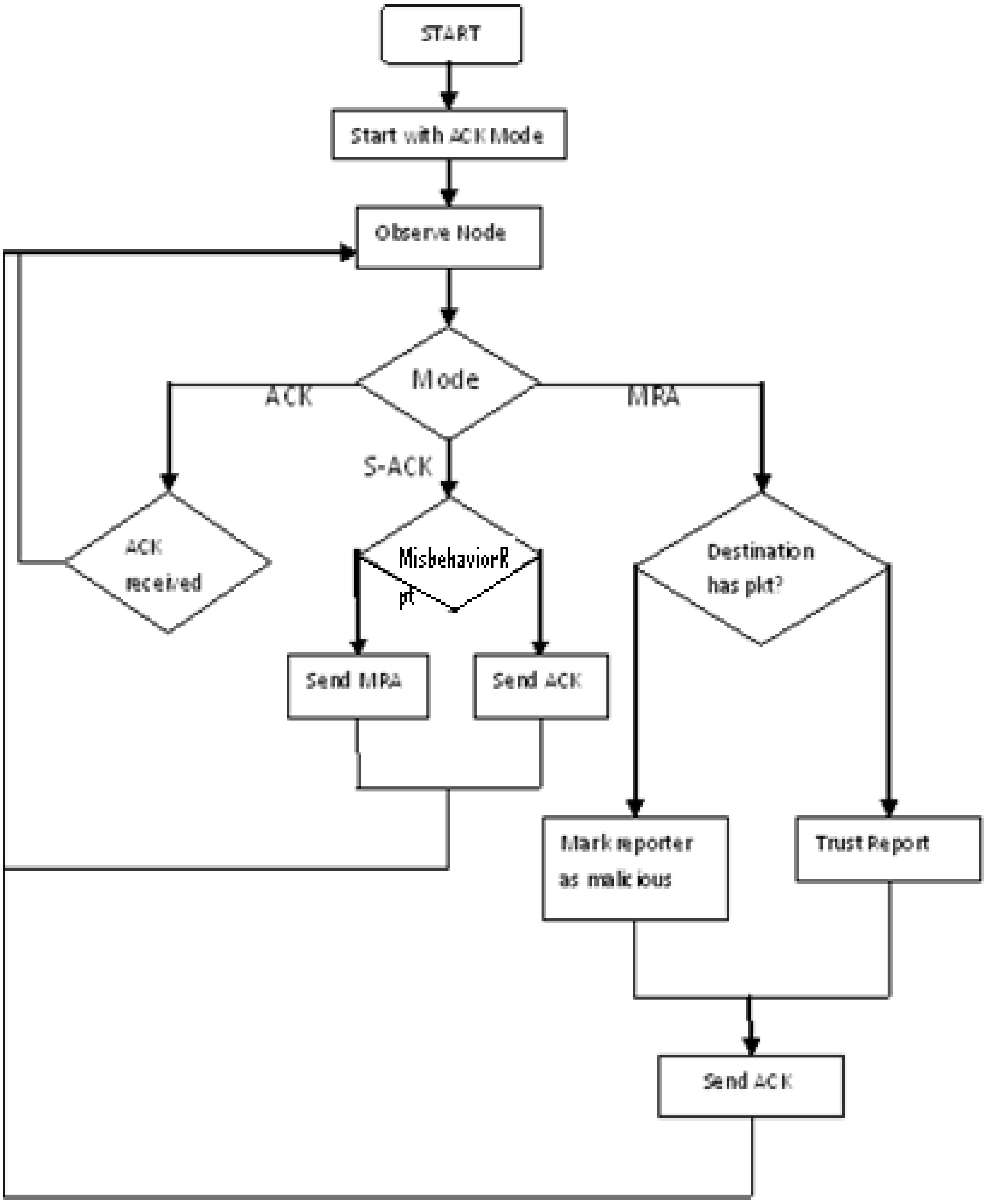


Figure 1: Overall CEAACK process

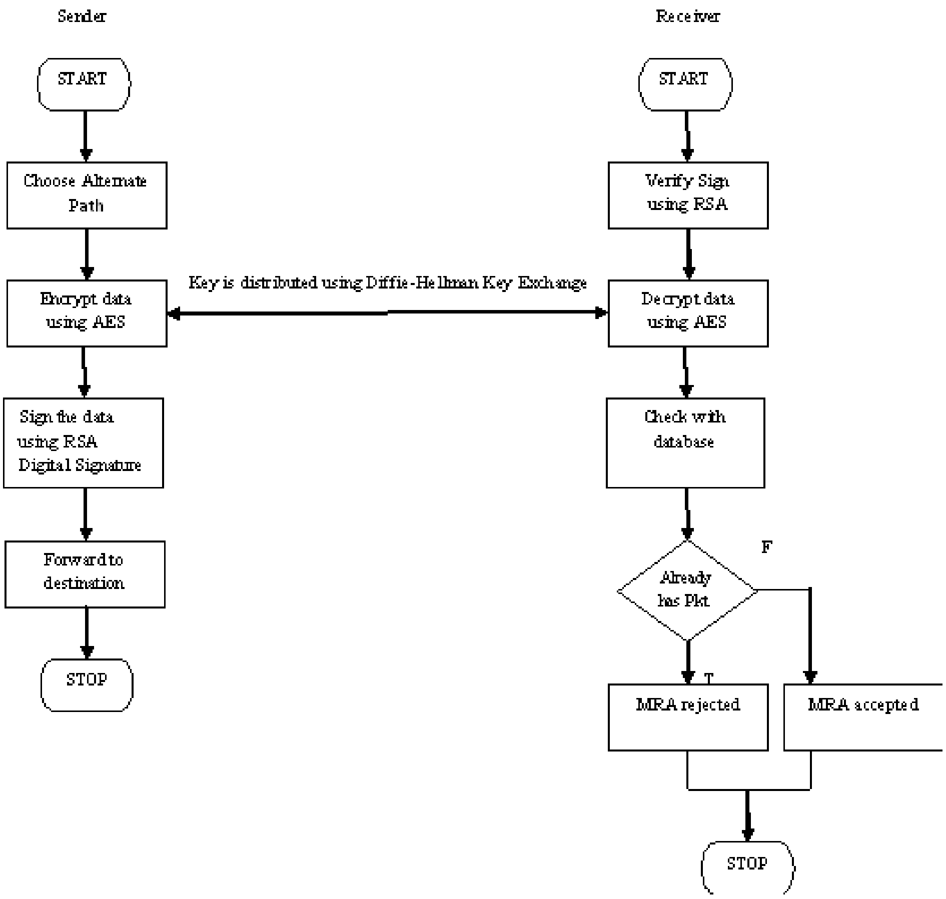


Figure 2: CEAACK -MRA Process

6. IMPLEMENTATION

CEAACK consists of three major parts, namely, ACK, Secure ACK (S-ACK), and Misbehavior Report Authentication (MRA).

Modules

It mainly contains 6 modules

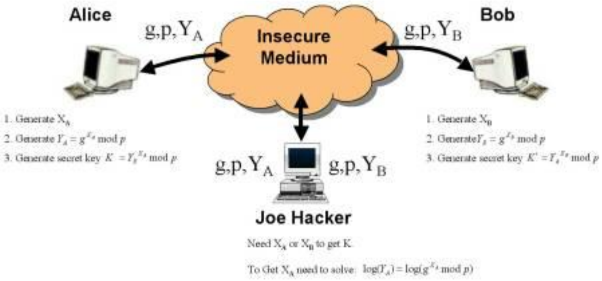
1. Network Formation
2. Key Exchange
3. Data Routing in MANET
4. CEAACK-ACK Module
5. CEAACK-SACK Process
6. CEAACK-MRA

Network Formation

In this module we can construct a topology to provide communication paths for wireless adhoc network. Here the node will give the own details such as Node ID through which the transmission is done and similarly give the neighbor nodes details. Each node has the routing table for update its local information.

Key Exchange

Diffie-Hellman key exchange [14] is used to distribute the secret key which is used in AES.


Alice
Bob
Insecure Medium
g,p,Y_A
g,p,Y_B
1. Generate X_A
2. Generate $Y_A = g^{X_A} \bmod p$
3. Generate secret key $K = Y_B^{X_A} \bmod p$
1. Generate X_B
2. Generate $Y_B = g^{X_B} \bmod p$
3. Generate secret key $K' = Y_A^{X_B} \bmod p$
g,p,Y_A
g,p,Y_B
Joe Hacker
Need X_A or X_B to get K
To Get X_A need to solve: $\log(Y_A) = \log(g^{X_A} \bmod p)$

Data Routing In MANET

In this module source node sends an encrypted message to destination, AES algorithm is been used, a hybrid cryptography technique is proposed for secure and authenticated data transmission. The message is signed by RSA Algorithm.

CEAACK- Acknowledgement Module

In this module the destination node sends acknowledgement details. All the packets including ACK packets are also signed by sender using RSA Algorithm. In this module nodes send acknowledgement packet who received the packet from the source.

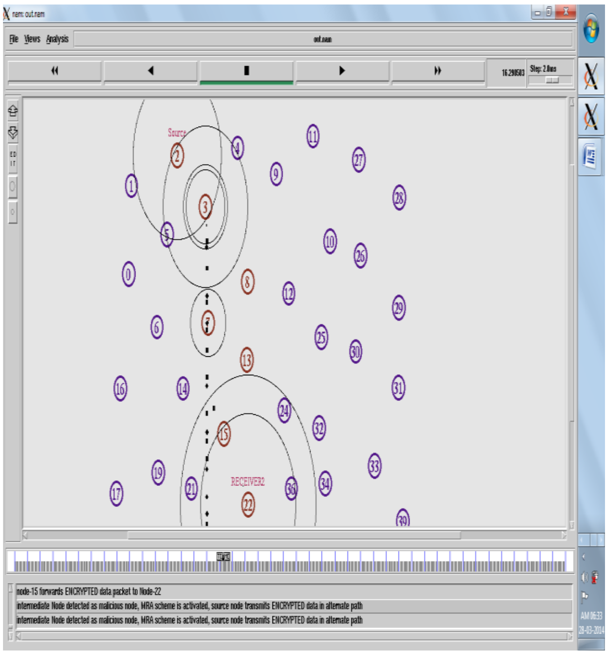
CEAACK – SACK PROCESS (ACK based ids)

If source node doesn't receives an ACK packet, then CEAACK results in secure acknowledgement process (SACK). The SACK [13] mode is a three consecutive intermediate node verification process. The first intermediate node sends a packet to second node and then to third node. The third node sends a ACK to second node, if the second node doesn't send ack to first one in predefined time, the first node generates a misbehavior report and send to source node stating second and third node are malicious node.

CEAACK – MRA (Misbehavior Report Authentication)
To initiate the MRA [13] 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 route exists, the source node starts a DSR (dynamic source routing) [11] routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. Source send encrypted & signed packet to destination via an alternate path. If the Receiver obtains the packet, it decrypts & verifies A’s originality & send ack. If the packet is a duplicate of already obtained packet then Report is malicious otherwise it is trusted.

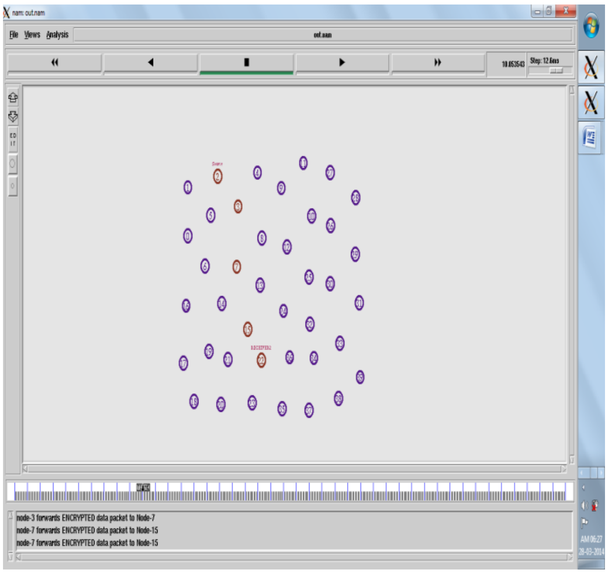
7. SAMPLE SCREEN SHOTS

Network Formation



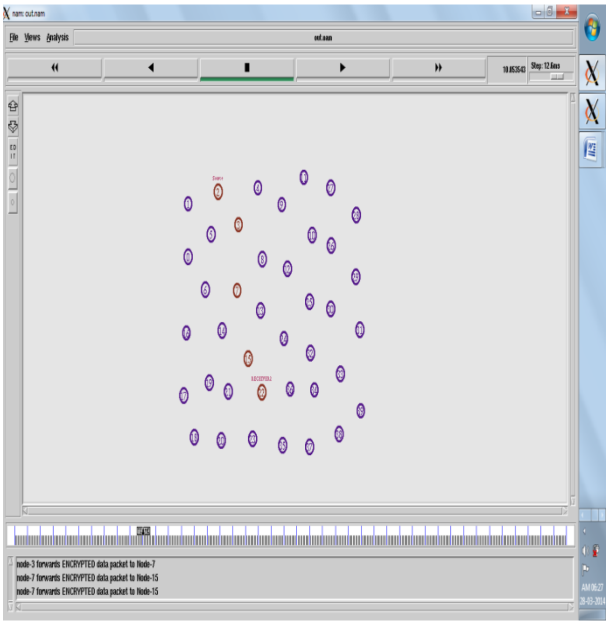
node-15 forwards ENCRYPTED data packet to Node-22
intermediate Node detected as malicious node, MRA scheme is activated, source node transmits ENCRYPTED data in alternate path
intermediate Node detected as malicious node, MRA scheme is activated, source node transmits ENCRYPTED data in alternate path

Data Routing



node-3 forwards ENCRYPTED data packet to Node-7
node-7 forwards ENCRYPTED data packet to Node-15
node-7 forwards ENCRYPTED data packet to Node-15

MRA Scheme



node-3 forwards ENCRYPTED data packet to Node-7
node-7 forwards ENCRYPTED data packet to Node-15
node-7 forwards ENCRYPTED data packet to Node-15

8. CONCLUTION AND FUTURE ENHANCEMENT

A major hazard to the security in MANETs is Packet dropping Attack. In this paper, we have proposed innovative IDS named CEAACK protocol specially designed for MANETs to overcome Packet-dropping attack. Here we used RSA Digital signature for signing data and AES algorithm for encrypting the data. Furthermore, in our system we used message digest cryptographic hash function to detect the malicious node anywhere in the network.

In future, we plan to adopt hybrid cryptography techniques to further reduce the network overhead caused by digital signature and testing the performance of CEAACK in real network environment instead of software simulation.

9. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in Wireless/Mobile Security. New York: Springer Verlag, 2008.

[5] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, “Modeling and optimization of a solar energy harvester system for self-powered.

[7] V. 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] Y. Hu, D. Johnson, and A. Perrig, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” inProc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

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

[10] G. Jayakumar and G. Gopinath, “Ad hocmobile wireless networks routing protocol—A review,” J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[11] 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.

[12] 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.

[13] Shakshuki, E.M.; Nan Kang; Sheltami, T.R., "EAACK—A Secure Intrusion-Detection System for MANETs," *Industrial Electronics, IEEE Transactions on* , vol.60, no.3, pp.1089,1098, March 2013.

[14] Ahmed Shihab, Alcahest; and Martin Langhammer, Altera, “Design How-To Implementing IKE Capabilities in FPGA Designs”.

[15] 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.

[16] 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.

[17] 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.

[18] http://www.webopedia.com/TERM/N/network_security.html