ISSN 2320 – 2602

Volume 4 No.4, April 2015

International Journal of Advances in Computer Science and Technology

Available Online at http://www.warse.org/ijacst/static/pdf/file/ijacst08442015.pdf

Adoption of Hybrid Cryptography in an Acknowledgement Based Intrusion Detection System for Manets

Deepa M[1], Parvathi M[2]

[1]PG Student, Nandha Engineering College, Erode, mm.deepa@gmail.com
[2]Associate Professor, Nandha Engineering College, Erode, mparvathicse@gmail.com

ABSTRACT

Mobile ad hoc network consists of mobile nodes where network topology and administrative domain membership can change rapidly. Thus it is important to provide security services such as network availability, confidentiality and integrity. In this paper, we propose a hybrid acknowledgement based intrusion detection system which exhibits higher malicious node detection with a minimal routing overhead and improves the network performance. In order to detect the forged acknowledgment, all the acknowledgement packets are ensured with digital signature. Due to larger key sizes of the conventional schemes, hybrid cryptography is implemented in such a way that it reduces the computational complexity, battery power and routing overhead. The popular symmetric encryption method such as AES provides a better security but maintenance of keys is tricky. Compared to the symmetric encryption schemes, key management is not complicated in asymmetric techniques but the extent of security is very less. To cope up with these shortcomings a new version of hybrid encryption is proposed which is a combination of Advanced Encryption Standard and Elliptic curve cryptography ECC for the acknowledgement packets.

Key Words: Hybrid, ECC, AES, Encryption, Cryptography, Acknowledgement

1 INTRODUCTION

Mobile ad hoc network is a collection of mobile nodes, which configures itself. The nodes itself act as a transmitter and receiver in the case of node communicating within the radio range. [1] [2].If two nodes are not within the radio range, communication takes place by forwarding packets with the cooperation of other nodes in the network. The open medium and remote distribution of MANET makes it vulnerable to various types of attacks. Therefore an intrusion detection system must be used to improve the security in MANET. Watchdog scheme is the most popular IDS described in the literature. Watchdog scheme [3] [4] [5] [6] [7][8] listens to its next hop transmission. If the node fails to forward the packet to the next hop, the watchdog increases the counter value. If the counter value exceeds the threshold value, it reports the node as malicious. Pathrater [7] works in collaboration with the routing protocols in path selection. In TWO ACK scheme, the misbehaving links can be detected. In this scheme, acknowledgement packets are transmitted for three consecutive nodes from source to destination. But the acknowledgement packet produces the network overhead which drastically reduces the network performance and consumes more battery power. .EAACK is the novel approach that provides solution to the preceding approaches by the combination of Digital signature.EAACK is an acknowledgement based IDS. EAACK scheme uses ACK, S-ACK and MRA acknowledgement based intrusion detection schemes. The significance of this scheme is to provide authenticated acknowledgements. So, that a digital signature is implemented in the EAACK scheme. Using the digital signature scheme, all acknowledgement packets are digitally signed before they are sent out, and verified until they are accepted. But the use of digital signature in the acknowledgements requires additional resource utilization.[9]

2 BACK GROUND

2.1 Functional Parts Of Enhanced Adaptive Acknowledgement IDS

The three main parts of the enhanced adaptive acknowledgement based IDS are ACK, secure ACK and false misbehaviour report authentication. This scheme uses the digital signature method to prevent the attacker from forging acknowledgment packets. Before the acknowledgement packets are sent out , the IDS requires all the acknowledgement packet to be signed [9].

2 .1.1 Acknowledgement Scheme

ACK is an end-to-end acknowledgement scheme. The intention is to reduce the network overhead when no network misbehaviour is detected. In the ACK mode, the node S sends the ACK data packet to the destination node D. After that, all the intermediate nodes between the source and destination are cooperative and once node D successfully receives the packet, it requires to send the ACK packet back to the node S with same route but in reverse order. If the acknowledgement packets are unsuccessful or if it does not reach the source on time, function will be performed to detect the misbehaving nodes. Figure1 shows the functional parts of the acknowledgment based IDS.

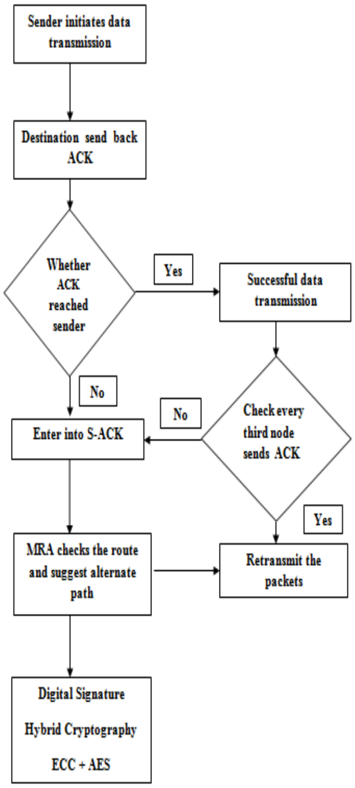
Sender initiates data transmission
Destination send back ACK
Whether ACK reached sender
Yes
Successful data transmission
No
No
Enter into S-ACK
Check every third node sends ACK
Yes
MRA checks the route and suggest alternate path
Retransmit the packets
Digital Signature
Hybrid Cryptography
ECC + AES

Figure 1. Functional parts of IDS

2.1.2 Secure Acknowledgement

In the secure acknowledgement scheme, to detect the misbehaving nodes every three successive nodes work in a group. In the three successive nodes the S-ACK acknowledgment packet is sent by the third node to the first node. The S-ACK scheme is able to detect the misbehaving nodes in the presence of receiver collision and low transmission power. In the S-ACK scheme the three consecutive nodes N1, N2, and N3 work as a group to identify the misbehaviour of the nodes. At the first node N1 sends the S-ACK packet to node N2. Then the node N2 forwards to node N3. After the node N3 receives the Packet it is responsible to send back acknowledgement packet S-ACK packets to node N2. Node N2 to N1. Within a predefined threshold time the node N1 does not receive the acknowledgement packet the node N2 and N3 are malicious nodes. This can be reported by N1 node and inform to the source node.

2.1.3 Misbehavior Report Authentication

The watchdog scheme fails to identify the misbehaving nodes due to the presence of a false misbehaviour report. To overcome this problem, the MRA scheme is used to authenticate whether the destination node has received the reported missing packet through a different route. If the reported node is received in an alternative route from source to destination, MRA will mark the node as innocent node. In further transmission process the node will be included otherwise ignored.

3 PROBLEM DESCRIPTION

The proposed scheme is a new and efficient acknowledgement based intrusion detection system specially designed for MANETs. Compared to conventional approaches, the proposed IDS demonstrates higher malicious behaviour detection rates in certain circumstances while does not greatly affect the network performance. In order to ensure the integrity of the intrusion detection system, the IDS requires digital signature for all acknowledgements before they are sent out and verified until they are accepted. Since the key sizes of RSA and DSA schemes which are used for generating the digital signature are very large, the routing overhead will be more. In order to reduce the routing overhead caused by digital signature, hybrid cryptography is introduced. Hybrid cryptography combines the ease of asymmetric key cryptography with the competence of symmetric key cryptography. Public key encryption is implemented for random symmetric key encryption. In the recipient side, public key encryption method is used to decrypt the symmetric key. Recovered symmetric key is used to decrypt the message.

4 SCHEME DESCRIPTION

The Advanced Encryption Standard has reached new heights in providing secure systems for the forthcoming years. The NIST standard demonstrates that ECC's public key sizes are perfectly equivalent with AES. So the hybrid combination of ECC and AES achieves greater competency by combining the ease of the two cryptosystems [13].

4.1 Hybrid Encryption Module

Hybrid encryption is the combination of Advanced Encryption Standard and Elliptic curve cryptography. AES algorithm is a very popular symmetric encryption algorithm which involves key sizes and block sizes. The key sizes and block sizes should be pre determined. In AES encryption method round transformation is performed as set of iterations which include sub bytes, shift rows, mix columns and add around key. In this scheme, the data and the signature are encrypted. Using the ECC encryption scheme, the private key of AES scheme is encrypted which generates a key cipher text. ECC encryption can be described as follows. Let us consider the elliptic curve equation E(x,y). Let G be the point on the elliptic curve.. The private keys are generated randomly. Public key is Q = kG. The plain text will be encoded to M bits of the curve which generates a random number r and C1 and C2. Using the unique private key of the receiver C1 and C2 can be decrypted. Since the key sizes of the AES scheme scales perfectly with the light weight public encryption scheme ECC, the system produces a good network performance. Figure 2 and Figure 3 explains the hybrid encryption and hybrid decryption modules in detail respectively.[12]

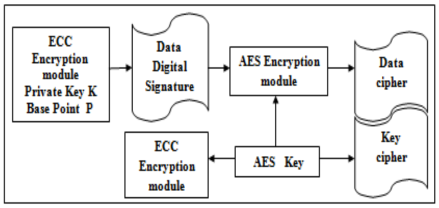

Figure 2 *Hybrid encryption module*

4.2 Hybrid Decryption Module

When the receiver receives the cipher text, the receiver uses his private key of the ECC decryption module to decrypt the key cipher and then uses the decrypted key for recovering the data cipher text and digital signature.

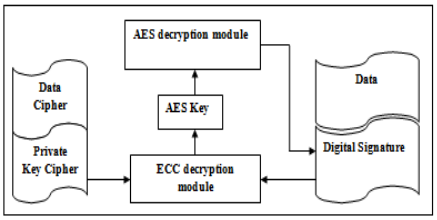

Figure 3 *Hybrid decryption module*

5 PERFORMANCE EVALUATION

5.1 Simulation Configuration

Simulation is conducted in ns 2,34 environment on Ubuntu 10.04. In order to measure the performance of the proposed scheme two performance metrics has been considered.

1) Packet delivery ratio -PDR defines the ratio of number of packets received by the destination to the number of packets sent from the source.

2) Routing overhead - RO defines the ratio of number of routing related transmissions like RREQ,RREP,ACK,ERR

5.2 Comparison Of Routing Overhead And Packet Delivery Ratio For Different Schemes.

In basic aodv model there is no ack sharing so overhead is very less, but in two-ack scheme there are number of acknowledgement shared between each node so network overhead is very high. AACK scheme cannot find forged acknowledgement packets. So packet delivery ratio is very less and the routing overhead is minimal. But EAACK and Hybrid ACK scheme can provide good performance in false acknowledgement scenario and normal malicious scenario. Since Hybrid ACK scheme uses Light weight public encryption scheme, the routing overhead caused is less compared to the existing schemes and delivers a good packet delivery ratio.

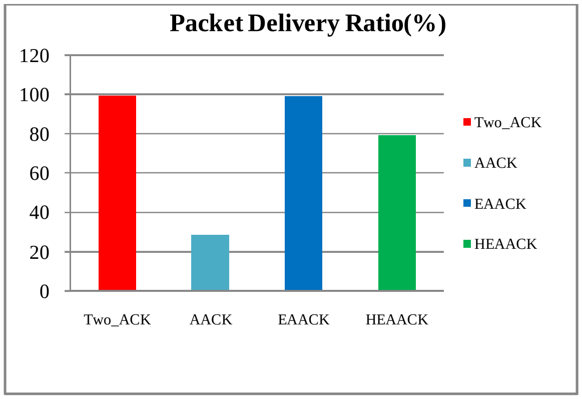

Figure 4 *Comparison of packet delivery ratio*

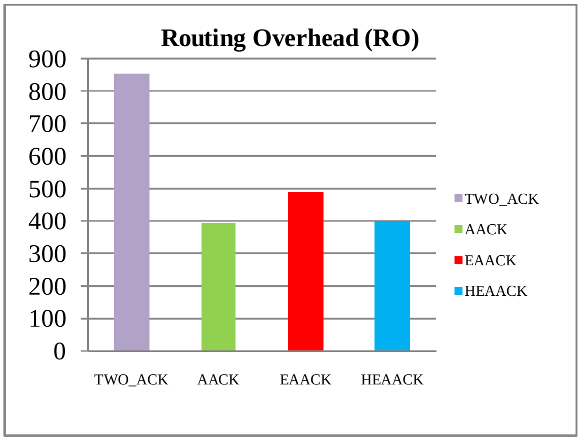

Figure 5 *Comparison of routing overhead*

6 CONCLUSION AND FUTURE WORK

The security sensitive applications of ad hoc networks like military applications require high degree of security, but ad hoc networks are vulnerable to various active and passive attacks like packet dropping attack. Elliptic curve cryptography provides an efficient alternative to RSA and DSA public key encryption scheme. Thus the combinatorial use of ECC and AES provides better security in an acknowledgement based intrusion detection system with the achievement of network performance. Thus it paves a great way in the reduction of the routing overhead compared to the existing scheme. Moreover hybrid acknowledgement based IDS requires Key Pre distribution.

1) In future Threshold cryptography can be applied to build a highly available and highly secure key management service by distributing trust among a group of servers rather than key pre distribution.[10] [11].

2) Also self contained public key management scheme can be used in acknowledgement based IDS rather than key pre distribution .So that near zero communication overhead can be achieved. [14]

REFERENCES

1. Mishra and K. M. Nadkarni, "**Security in wireless ad hoc networks – A Survey**", in The Handbook of Ad Hoc Wireless Networks, M. Ilyas, Ed. Boca Raton: CRC Press, 2002, pp. 30.1-30.51.

2. P. Papadimitratos and Z. Hass, "**Securing Mobile Ad Hoc Networks**", in The Handbook of Ad Hoc Wireless Networks, M. Ilyas, Ed. Boca Raton: CRC Press, 2002, pp. 31.1-31.17

3. S. Marti, T. Giuli, K. Lai, and M. Baker, **―Mitigating Routing Misbehavior in Mobile Ad Hoc Networks**, Proc. MobiCom, Aug. 2000.

4. 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.

5. J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "**On intrusion detection and response for mobile ad hoc networks**," in Proc. IEEE Int. Conf.Perform., Comput., Commun., 2004, pp. 747–752.

6. A. Patcha and A. Mishra, "**Collaborative security architecture for black hole attack prevention in mobile ad hoc networks**," in Proc. Radio Wireless Conf., 2003, pp. 75–78.

7. Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. **Mitigating routing misbehavior in mobile ad hoc networks**. In Mo-biCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pages 255_265, New York, NY, USA, 2000. ACM.

8. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "**An acknowledgment-based approach for the detection of routing misbehavior in MANETs**," IEEE Transactions Mobile Computing, vol. 6, no. 5, pp. 536–550, May 2007.

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

10. Y. G. Desmedt, "**Threshold cryptography**", European Transactions On Telecommunications, 5(4), pp. 449-457, July-August 1994.

11. P. S.Gemmell, "**An Introduction to Threshold Cryptography**", Cryptobytes,1997, pp.7-12.

12. K. Lauter, "**The advantages of Elliptic Curve Cryptography For Wireless Security**", IEEE Wireless Communications, vol. 11, no. 1, Feb. 2004, pp. 62-67

13. Bing Ji, Liejun Wang,Qhing hua Yang,"**New Version Of AES-ECC Encryption System Based on FGPAin WSNs**.", Journal of Software Engineering 9(1):87-95,2014

14. L. Eschenauer, V.D. Gligor, **A key-management scheme for distributed sensor networks**, in: ACM CCS '02, 2002, pp. 41–47