Volume : 2 | Issue : 11 | Nov 2013 • ISSN No 2277 - 8160

Research Paper | Engineering

Reducing Network Overhead in Mobile Ad-hoc Network Using Hybrid cryptography techniques

Sangeetha M — Assistant Professor, Department of Computer Science and Engineering, Engineering College, Namakkal, Tamilnadu, India

Vijayakumar R — Department of Computer Science and Engineering, Muthayammal Engineering College, Namakkal, Tamilnadu, India

ABSTRACT

Now a day we used many applications based on the mobility and scalability. Among all the up to date wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. MANET consists of mobile nodes which are free to move arbitrarily. MANETs are highly vulnerable for passive and active attacks because of their open medium, rapidly changing topology, lack of centralized monitoring. Both of the TWOACK and Watchdog methods solutions, which are considered as the first line of defense, are not sufficient to protect MANETs from packet dropping attacks. And the new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. But this technique also having some potential issues like network overhead, collusion and partial dropping. In this paper, we propose and implement a new technique called Hybrid cryptography specially designed for reduce network overhead. Due to this, it improves network performance.

KEYWORDS : Mobile Ad hoc NETwork, Hybrid cryptography, Security

1. INTRODUCTION

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular devices, etc have to reduce significantly. Several versions of wireless networks have emerged in order to concentrate on the needs of both business and personality users. One of the most established versions of wireless networks is the Wireless Local Area Network (WLAN). WLANs have a short range and are usually deployed in places such universities, industries, cafeteria, etc. However, there is still a need for communication in a number of scenarios of employment where it is not sufficient to deploy fixed wireless access points appropriate to objective constraints of the medium. In this case, it is not only feasible to deploy a fixed wireless access point, but also risky since an enemy attack would bring downwards the total network. This difficulty has led to a rising interest among the investigate area in mobile ad hoc networks (MANETs), wireless networks comprised of mobile computing devices communicate without having any fixed infrastructure.

2. NETWORK MODEL

2.1 INTRUSION DETECTION SYSTEM (IDS) ARCHITECTURE

MANET has features such as an open medium, dynamic changing topology, and the lack of a centralized monitoring and management point, many of the intrusion finding techniques residential for a fixed wired network are not applicable in MANET. Zhang [3] gives a specific design of intrusion finding and reaction mechanisms for MANET. Marti [4] proposes two mechanisms: watchdog and path rater, which improve throughput in MANET in the presence of nodes that agree to forward packets but fail to do so. Intrusion Detection Techniques for Node Cooperation In MANETs: Since there is no infrastructure in mobile ad hoc networks, every node should rely on other nodes for collaboration in routing and forward packets to the destination.

Fig.2.1. Intrusion Detection System (IDS)

2.2 NETWORK OVERHEAD

Network overhead is an main concept to understand. Understanding overhead is basic to understanding the methodology employed by various technologies to get information from one place to another, and the costs involved.

3. EXISTING SYSTEM

In MANET uses the EAACK[8] technique for handling three of the previous failures of watchdog. And also provide network performance.

In this section, we mainly describe three existing approaches, namely,

1. Acknowledgment (ACK),
2. Secure-Acknowledgment (S-ACK) and
3. Misbehavior Report Authentication (MRA).

3.1 ACKnowledgment

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 misbehavior is detected. In ACK mode, node S first sends out an ACK data packet Pad1 to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order.

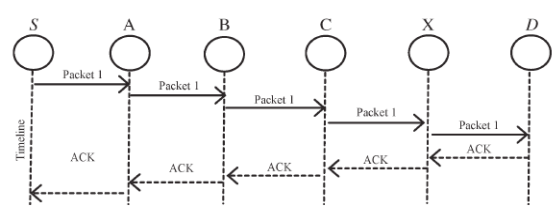

Fig.3.1. ACK scheme

3.2 Secure-ACKnowledgment

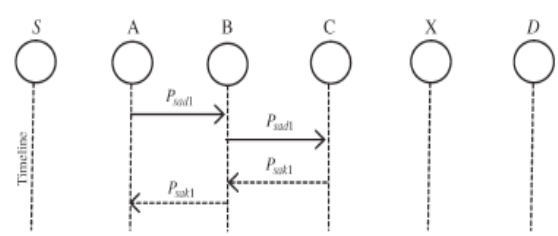

Fig.3.2. S-ACK

3.3 Misbehavior Report Authentication

When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehavior report and whoever generated this report is marked as malicious. Or else, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report. Since discussed earlier,

EAACK is an acknowledgment-based Intrusion Detection System.

All three parts of EAACK, that is, ACK, S-ACK, and MRA, are acknowledgment-based detection scheme. They all rely on response packets to discover misbehaviors in the network. Hence, it is really important to ensure to everyone acknowledgment packets in EAACK are authentic and untainted. If not, if the attackers are smart sufficient to forge acknowledgment packets, all of the three schemes will be vulnerable. However, we fully understand the extra resources that are required with the beginning of digital signature in MANETs. To address this concern, we implemented both DSA [10] and RSA [11] digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

4. PROPOSED SYSTEM

In this paper, we propose a hybrid cryptography technique to reduce the network overhead caused by digital signature. Some times more malicious nodes are present in the network. In more malicious nodes require more acknowledgement packets. At that time the ratio of digital signature in the whole network overhead. In the presence of malicious nodes, routing overhead reduced by any hybrid techniques [12]. We propose a hybrid technique by using RSA and AES. In this research work, first we find out the secure route for data transmission. On one occasion the source node receives the RREP, it may begin to forward data packets to the destination. Based on this protocol, the destination is required to send a reply message to the corresponding sender. After getting a secure route, send a data securely to the destination by using hybrid encryption techniques. The data send from the source node will be encrypted with RSA and AES before its travelling to the destination node. Before receiving the data to the destination node that is decrypted with RSA and AES.

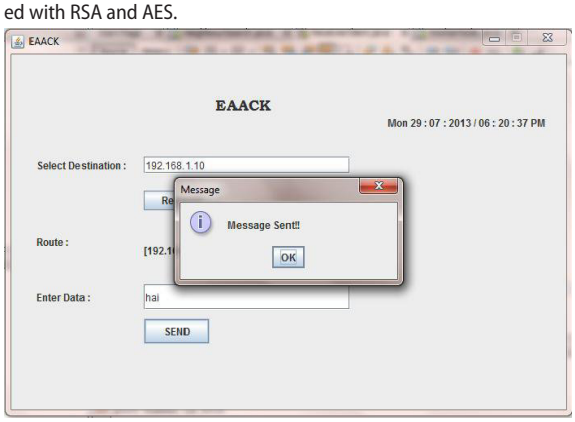

Fig.4.1. Sender can receive an acknowledgement packet with presence of non malicious node.

At the destination node the data will be available on decryption. After receiving the data at destination, the destination node required to send an acknowledgement packet to the source.

In the presence of malicious node, the destination node is not received the data from the source. Because the sender node cannot be identifies the route to the destination.

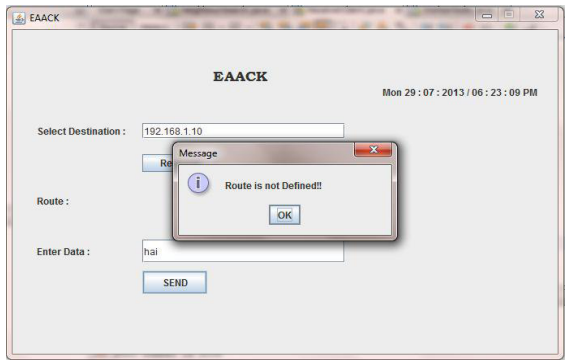

Fig.4.2. In the presence of malicious node, the sender cannot define the route. So that routing overhead is reduced in hybrid technique.

The hybrid cryptography technique is used to reduce overall network overhead and increase the network performance. The overall graph for increase Quality of service(QoS) and decrease the network overhead is shown in below figure.

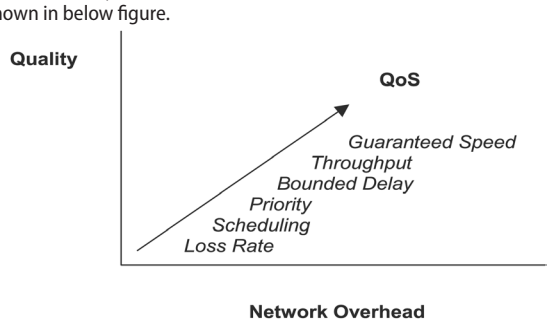

Fig.4.3. performance for network quality

5. CONCLUSION AND FUTURE WORK

An effort to prevent the attackers from initiate forged acknowledgment attacks, we comprehensive our research to incorporate hybrid cryptography technique in our proposed scheme, it can reduce the routing overhead in the network.

- To make bigger the merits of our research work, we plan to examine the following issues in our future research:
- To avoid or minimize partial Packet-dropping in misbehavior in network communication.
- To adopting a key exchange mechanism to eliminate the requirement of predistributed keys.

REFERENCES

[1] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007. | [2] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007. | [3] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003. | [4] O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks,"Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p.57.1, January 2003. | [5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), pp.255-265, August 2000. | [6] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes -Fairness In Dynamic Ad-hoc NeTworks)," Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp.226-336, June 2002. | [7] P. Michiardi and R. Molva, Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," Communication and Multimedia Security Conference (CMS'02), September 2002. | [8] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami "EAACK—A Secure Intrusion-Detection System for MANETs," Transactions on Industrial Electronics, vol.60, no.3 pp. 1089– 1098, 2013. | [9] Jin-Shyan Lee, "A Petri Net Design of Command Filters for Semiautonomous Mobile Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 4, pp. 1835-1841, April 2008. | [10] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS). |