ISSN:2320-0790

An International Journal of Advanced Computer Technology

ECDSA - Performance improvements of intrusion detection in Mobile Ad-hoc Networks

Vijayakumar R[#1], Raja S[#2], Prabakaran M[#3]

[#]Department of Computer Science and Engineering,
Muthayammal Engineering College, Namakkal,
Tamilnadu, India

Abstract - A MANET is a temporary either single hop or multi-hop wireless network with collection of mobile nodes without an underlying infrastructure. In this network, the occurrences of misbehavior nodes are a main problem that degrades the network performance. In previous technique watchdog is used to detect nodes misbehaviors in the mobile ad-hoc network, but it contains some of potential issues. To avoid these issues we propose a novel algorithm named as Elliptic Curve Digital Signature Algorithm (ECDSA) particularly designed for increases the security in network.

Keywords - elliptic curve cryptography, DSA, ECDSA.

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 phones, etc have reduced drastically. Several standards for wireless networks have emerged in order to address the needs of both industrial and individual users. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN) [1]. WLANs have a short range and are usually deployed in places such universities, companies, cafeterias, etc. However, there is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical 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 down the whole network. This problem has led to a growing interest among the research community in mobile ad hoc networks (MANETs), wireless networks comprised of mobile computing devices communicating without any fixed infrastructure.

1.1 MOBILE ADHOC NETWORK

In last few years ad-hoc networking has attracted a lot of research interest. This has led to creation of a working group at the IETF that is focusing on mobile ad-hoc networking, called MANET (MANET, 2002). These networks should be mobile and use wireless communications.

Due to the popularity of mobile devices and independence from the infrastructure, a MANET can find wide applications in temporary wireless networks in meeting rooms, airports, and stadiums. It is fast, convenient, and economical to set up a MANET in a battlefield and for search and rescue. A Vehicular Ad-hoc Network, is variation of MANET, connects the running cars and fixed traffic lights and other sensors, is vital to implementation of smart transportation.

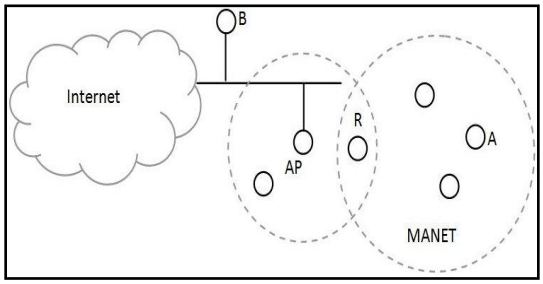

Fig.1.1. Mobile Ad-hoc NETwork (MANET)

Before the application of such an IP-based network, IP address assignment is one of the most important network configuration parameters for the mobile nodes. Without a valid unique IP address, a mobile node cannot participate in unicast communications. It can only receive and send broadcast messages,

which consumes valuable bandwidth and power, and thus it is desirable to limit the duration and scope of broadcast communications in a MANET.

For a small-scale MANET or a closed MANET, it may be simple to assign IP addresses to mobiles node by hand. It is also possible to burn an IP address in the ROM of a mobile node to re-use it repeatedly. However, the procedure will become inefficient and even impractical for a large-scale system or an open system where different kinds of nodes (such as laptops, smart phones, tablets, PDAs, and specialized computers) are free to join and leave.
Automatic IP address allocation is far more difficult to implement in a MANET than a hardwired network such as a local area network, due to instability of mobile nodes, multi-hop transmission of messages, openness of the system, and lack of infrastructure. Therefore, although DHCP or SAA is popular for hardwired networks, they cannot be directly ported to a MANET. A distributed algorithm that adapts to node mobility and topology change is more desirable.

1.2 ADVANTAGES OF MOBILE AD-HOC NETWORKS

Having discussed the general issues in MANETs, the reason behind their popularity and their benefits will now be discussed.

Instant infrastructure- Unplanned meetings, spontaneous interpersonal communications etc. cannot rely on any infrastructure
Disaster relief- Infrastructures typically break down in disaster areas
Remote areas- Depending on the communication pattern, ad-hoc networks or satellite infrastructures can be a solution
Effectiveness- It also provide a better & effective solution

2. EXISTING SYSTEM

If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches [2].
In this section, we mainly describe the existing approach namely, Watchdog.

2.1 WATCHDOG

In Marti et al., [3] proposed a reputation-based scheme. Two modules called watchdog and pathrater are implemented at each node, to detect and mitigate, respectively, routing misbehaviors in MANETs. Nodes operate in a promiscuous mode wherein, the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet or not. At the same time, it maintains a buffer of recently sent packets.

A data packet is cleared from the buffer when the watchdog overhears the same packet being forwarded by the next hop node over the medium. If a data packet remains in the buffer too long, the watchdog module accuses the next-hop neighbor to be misbehaving. Thus, the watchdog enables misbehavior detection at the forwarding level as well as the link level. Based on watchdog's accusations, the pathrater rates every path in its cache and subsequently chooses the path that best avoids misbehaving nodes.

Dynamic Source Routing protocol (DSR) is chosen for the discussion to explain the concepts of Watchdog and Path rater. The watchdog method detects misbehaving nodes. The watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop. A path rater then helps to find the routes that do not contain those misbehaving nodes. In DSR, the routing information is defined at the source node. This routing information is passed together with the message through intermediate nodes until it reaches the destination. Therefore, each intermediate node in the path should know who the next hop node is. Below fig.2.1 shows how the watchdog works.

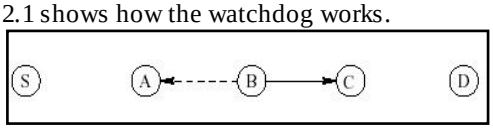

Fig.2.1. How watchdog works

Marti *et al.*, proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. 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. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme [4], [5].
Nevertheless, as pointed out by Marti *et al.*, the Watchdog scheme fails to detect malicious misbehaviors with the presence of the following:

1) ambiguous collisions

2) receiver collisions
3) limited transmission power
4) false misbehavior report
5) collusion
6) partial dropping.

3. PROPOSED WORK

The main problem of existing work is collision, low security and data dropping. This can be solved by using Elliptic Curve Digital Signature Algorithm (ECDSA). The ECDSA [6] is specified in ANSX9.62, as adopted for the computation of digital signatures in FIPS 186. ECDSA is normally specifies a minimum key size of 163bits.
The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the DSA. ECDSA was first proposed in 1992 by Scott Vanstone in response to NIST's (National Institute of Standards and Technology) request for public comments on their first proposal for DSS. The ANSI X9.62 ECDSA, present rationale for some of the design decisions, and discuss related security, implementation, and interoperability issues.

ECDSA key size (bits)	RSA key size (bits)	Key size Ratio
163	1,024	1:6
256	3,072	1:12
384	7,680	1:20
512	15,360	1:30

Fig.3.1: Key size comparison of ECDSA with RSA

The encryption and decryption process can be handled by DSA [7]. The ECDSA can be used to minimize the encrypted data size and also it uses the minimum key size compare to RSA [8] algorithm. The size is minimizing so the data dropping can be also minimized. The collision also reduced and security will be increased.

The ECDSA key size is very low compare than RSA that is shown in figure 3.1. So the dropping of data will be reduced due to minimum encryption data size and key size. In sender side the data will be encrypted and also digitally signed before data sent out. In receiver side the data will be decrypted at the same time data is digitally verified by receiver.

4. CONCLUSION AND FUTURE WORK

This ECDSA algorithm can provide less collision compare than watchdog technique. Packet dropping attack is a major risk to the security in MANETs. In ECDSA is also provided low packet dropping in data transmission. The DSA algorithm is efficient to prevent malicious nodes from attackers.
In future work, find out new algorithm for identify the false misbehavior report. And it's also testing the performance of ECDSA in real network environment instead of software simulation.

REFERENCES

[1] 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.

[2] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[3] 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.

[4] 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.

[5] 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.

[6] Aqeel Khalique, Kuldip Singh and Sandeep Sood "Implementation of Elliptic Curve Digital Signature Algorithm," International Journal of Computer Applications, Volume 2 – No.2, pp. 21– 27, May 2010.

[7] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[8] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.