IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-6, Jun 2019 E-ISSN: 2347-2693

Node Authentication in MANET by using Digital Group Signature with Elliptic Curve Cryptography

Atul Dubey

Department of Information Technology, Technocrats Institute of Technology, Bhopal, India

Corresponding Author: atulindia88@gmail.com, Tel.: +91-9827729433

DOI: https://doi.org/10.26438/ijcse/v7i6.261265 | Available online at: www.ijcseonline.org

Accepted: 10/Jun/2019, Published: 30/Jun/2019

Abstract— Security in the mobile ad hoc network is very challenging task due the open communication, absence of centralized control and authentication mechanism. In order to handle these security and reliability issues in the MANET (Mobile Ad hoc Networks), we have proposed a group digital signature and elective curve cryptography based modified AODV (Ad hoc On Demand Distance Vector Routing) routing protocol which provides authentication and reliable communication. Proposed digital group signature method has group manager which has administrative properties like to regulate the authentication mechanism and to handle the dispute or unauthorized node and it is able to check and verify the other node authenticity. We have tested our method on the basis of packet delivery ration, network throughput and the network load. Our approach will increase the transmission reliability and reduces the packet loss chance in comparison to existing approaches

Keywords— Ad-hoc networks; Security; Digital group signature; Elliptic curve cryptography; Node authentication; AODV.

I. INTRODUCTION

Mobile ad hoc network is very popular and has life saving application for search and rescue operation in the disaster, in military operations and area where the fixed networks are not possible. Because of these crucial applications it becomes more important to maintain reliable and secure communication. On the other hand security in the mobile adhoc network is more is very challenging task because MANET[1] does not has any centralized control mechanism and nodes are communicate in the open air. Along with these issues there is no authentication mechanism, therefore it is highly vulnerable to the attack[7][8]. Any malicious node can easily penetrate the security and it can easily perform malicious activity and steel the confidential information [9].

AOMDV uses the routing information already available in the basic AODV protocol, thereby reducing the overhead caused while discovering multiple paths [1].

Elliptic Curve Cryptography (ECC) is used to describe a group of cryptographic tools and protocols where the security is based on the discrete logarithm problem. ECC is based on sets of numbers and equations that are associated with elliptic curves [1].

Various attack are present in the MANET such as wormhole attack, sink hole, flooding attack, routing table overflow attack, Denial of Service (DoS)[2-4], and black hole [7]. MANET is more vulnerable to these attacks because nodes are communicates on the mutual trust and any node can join the network without any permission and restriction [14].

In this paper, we have proposed a new approach to address the security issues in the mobile ad-hoc network (MANET) [4] as shown in the figure 1. In the proposed method standard AOMDV [1] routing protocol is modified, Elliptic curve cryptography and digital group signature functionality introduces additionally in the routing protocol to improved security and privacy in the network. The proposed digital group signature based algorithm provides the secure access of the network. It overcome the problem of node authentication in the mobile ad hoc network and provides the access control over the malicious node.

The rest of the paper is organized as follows: Section II discusses various literatures proposed and contributions by various authors. Section III describes the proposed methodology and discusses digital group signatures. Section IV gives the implementation details and the various results. Section V concludes the research and Section VI proposes future works.

II. RELATED WORK

Sultana et al. [1] proposed a system for black hole attack to study the performance of they consider AOMDV protocol. For securing network connections, Elliptic curve Cryptography technique is used. N Chaitanya Kumaret [2] et al. proposed a Protective secret sharing for long lived MANET Using Elliptic curve cryptography. Elbasher Elmahdi, Seong-Moo Yoo and Kumar Sharshembiev,[3] 2018 securing data forwarding against black hole attacks in mobile Ad-hoc network.Amit Kumar Yogi [4] et al. proposed an implementation of modified AOMDV routing protocol in different wireless network.

H. S. Chiu and K.S. Lue [5] introduced a method to detect both hidden and exposed wormhole attacks. In DELPHI, the sender gets all the disjoint paths between a sender and a receiver. After that, sender calculates the number of hops count and delay for each hop, the information is used to detect the wormhole attacks in the network. A path that has wormhole links will have a larger delay per hop value. X. Wang and J. Wong [6] proposed an end-to-end detection of Sybil attack (EDWA) in mobile ad-hoc networks. In this method detection of Sybil made based on hop count if hop count is very less compared to establish count then that path has Sybil attack. The result of detection is broadcast into the network to aware the other nodes in the network. After detection and identification of the Sybil the source node could select a shortest path from the set of legalize paths. The main drawback of this method is that it does not work well when the source and destination are too far away.

M. natu and A. Sethi [7] proposed an intrusion detection system to detect a wormhole using fault location techniques to defend against wormhole attack. Passive monitoring, proving, and event correlation tools have used to detect wormhole attacks in the network. In this method, two types of anomalies have focused to identify the nodes involved in a wormhole attack: end-to-end

III. PROPOSED RESEARCH METHODOLOGY

In this research work, we have proposed a new approach to address the security issues in the mobile ad-hoc network (MANET) [4]. In the proposed method, standard AOMDV (Ad hoc On Demand Multiple Path Distance Vector Routing) [1] routing protocol is modified, Elliptic curve cryptography and digital group signature functionality introduces additionally in the routing protocol to improved security and privacy in the network.

The proposed digital group signature based algorithm provides the secure access of the network. It overcome the problem of node authentication in the mobile ad hoc network and provides the access control over the malicious node. In figure1 depicted the block diagram of the proposed algorithm framework. As we can seen our proposed method is integrate with AOMDV [1] routing protocol.

A. DIGITAL GROUP SIGNATURE

Digital group signature is a public key based signature technique which has additional privacy and security features. In this technique, all network node form a group, and all nodes (group member) has its own private and group public key. Node signs the message before transmission. Anyone of the node can verify this sign. If the signature is valid, it means node genuine and eligible for communication in the network otherwise case is reported to the group manager (GM). The group manager is a special member node which handles dispute related to the signature validation. There is some algorithm in the group signature scheme as following:

1. Setup: For the initialization and generation of the private and group public key this algorithm is run by the Group manager.
2. Join: when a new node joins the network, then group manager run the join algorithm which produces group public membership key and user`s secret membership key.
3. Sign: Each node for generating the signature runs sign algorithm. This algorithm took a message, group public key and the private key of the node as input.
4. Verify: Receiver node run this algorithm to validate the signature.
5. Open: In case of the dispute occur in the signature, GM run this algorithm to handle the problem.
6. Revoke: Group manager run this algorithm to remove any node, or to assign new group public key

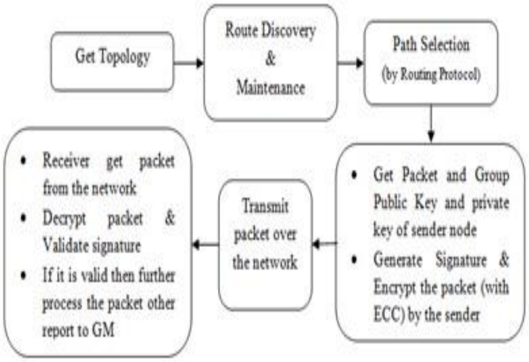

Get Topology
Route Discovery & Maintenance
Path Selection (by Routing Protocol)
Get Packet and Group Public Key and private key of sender node
Generate Signature & Encrypt the packet (with ECC) by the sender
Transmit packet over the network
Receiver get packet from the network
Decrypt packet & Validate signature
If it is valid then further process the packet other report to GM

Figure1 - Block diagram of proposed methodology

Digital group signature method is combined with the routing protocol which provides authentication capabilities in the mobile ad hoc network as shown in the data flow diagram in the figure 2. Steps involve in the digital signature and validation is described in the following section:

AT Sender:

Get packet from the host, network public key and private key of the sender.

Compute digital signature by calling Sign procedure, packet and network public key (group public key) and private key passed as parameter to the Sign procedure.

Apply Elliptic curve cryptography to get the encrypted packet.

Sent packet into the selected route by the AOMDV [1] routing protocol.

AT Receiver:

Receiver node receive packet from the network.

Decrypt the packet by the ECC decryption algorithm.

Check and validate the digital signature of the sender.

```
IF it is valid signature then establish connection for the further communication.
Else
Discard the packet, stop communication and report to Group manager (GM). GM inform to all other node in the network about the malicious node.
    EndIF
```

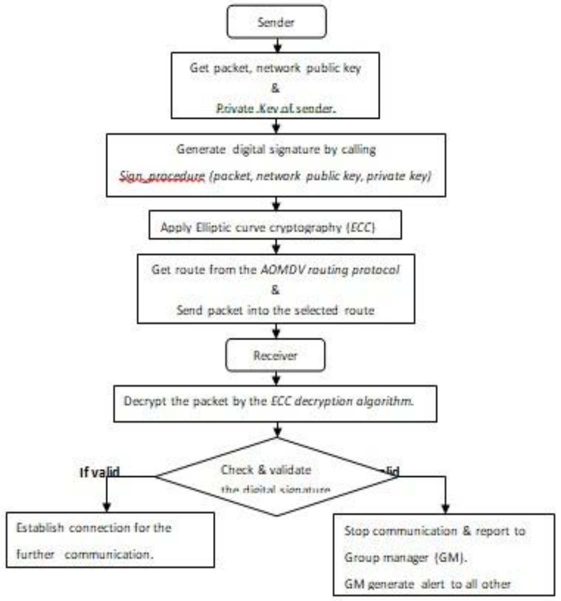

Sender
Get packet, network public key
&
Private Key of sender.
Generate digital signature by calling
Sign_procedure (packet, network public key, private key)
Apply Elliptic curve cryptography (ECC)
Get route from the AOMDV routing protocol
&
Send packet into the selected route
Receiver
Decrypt the packet by the ECC decryption algorithm.
Check & validate
the digital signature
If valid
lid
Establish connection for the
further communication.
Stop communication & report to
Group manager (GM).
GM generate alert to all other

Figure 2: Data flow diagram of proposed algorithm.

IV. IMPLEMENTATION AND SIMULATION RESULT

Simulation is performing on network simulator (NS-2), NS-2 is powerful research tool for wireless network such as MANETs. In simulation 30 nodes are used, time simulation time is 100 second and AODV routing protocols is used as the routing protocol and for implementing proposed method AODV protocol is modified. Performance is measure in on the base of network throughput, packet drop rate, end to end packet delay, packet delivery fraction percentage.

TABLE 1. SIMULATION ENVIRONMENT

Simulation Parameter	**Values**
Simulator Used	NS-2.35
No of Node	30
Routing Protocol	AODV
Simulation Time	100sec
Traffic Type(TCP/UDP)	1KB
Antenna Height	150m

A. *Result Discussion*

Results are evaluated of original AODV and proposed rate control scheme with MAODV. In order packet delivery scheme is implemented and performance analysis of proposed method is measures on the following parameters discussed here.

1). Packet Delivery Ratio (PDR) Analysis

Packet delivery ration is ratio between the successfully packet received to packet transmitted in the network. The comparison between exiting work and proposed work is shown in the figure 3. In the figure we can observed that PDR is better for the proposed method.

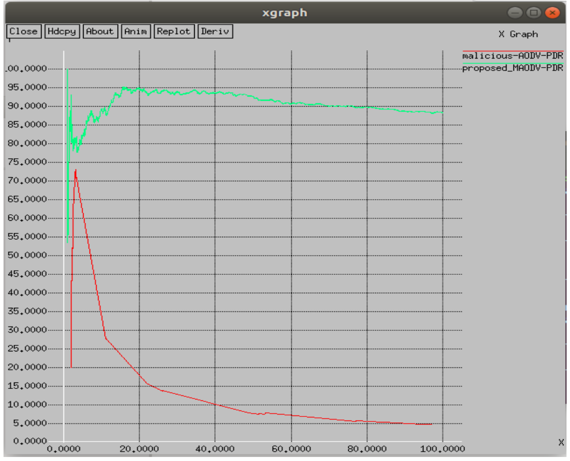


Figure 3: PDR Analysis

2). Routing Load Analysis

Number of packets required for management of routing is called routing load. For route management such as route discovery and to maintain router required to communicate with node by using extra packets. Figure 4 shows the comparison between exiting and proposed work.

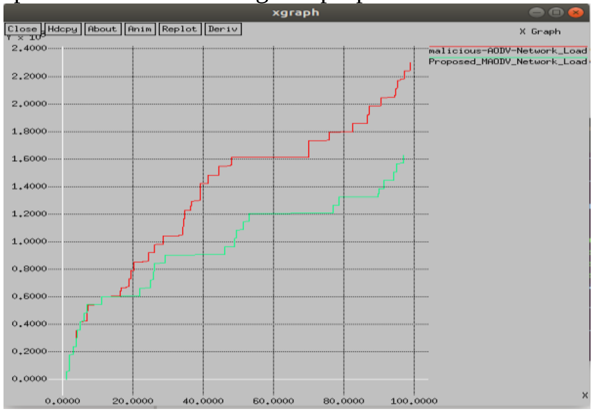


Figure 4: Routing Load Analysis

3). Throughput Analysis

Successful packets received by receiver in per unit time is called network throughput. The throughput analysis in this research is measured in number of packets transmitted per second in the network. The throughput is shown in figure 5. and graph shows the better results in case of proposed algorithm based method with compare to existing method.

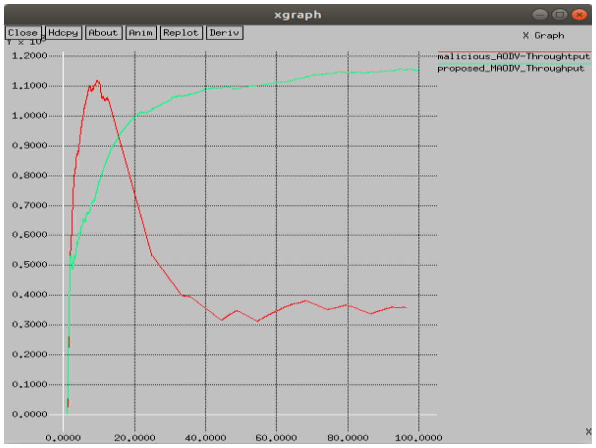
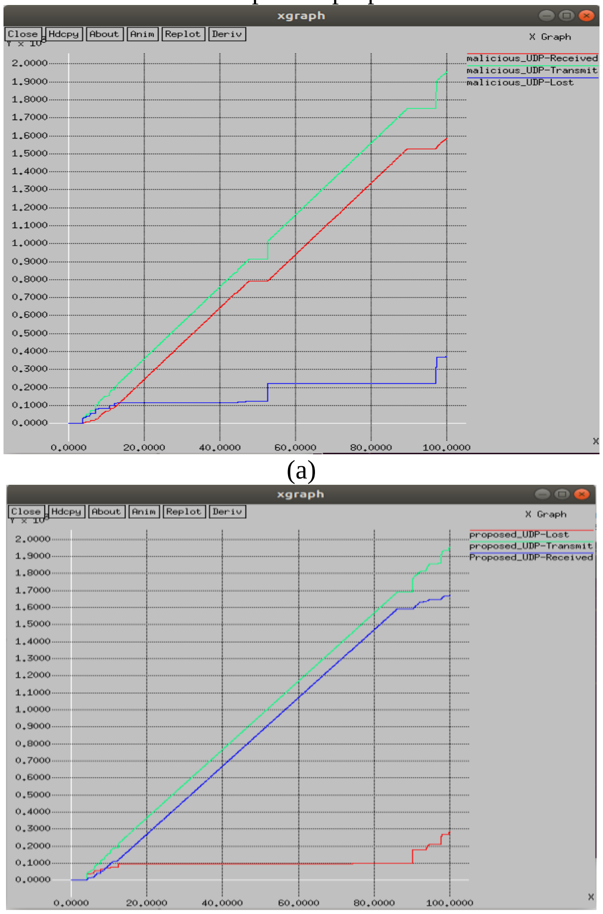


Figure 5: Throughput Analysis

4). UDP packet Analysis

In the figure 6 a and figure 6 b shows the UDP packet analysis in the suspicious (malicious node) network as well as in the proposed group digital signature based network. In the figure we can see that packet loss in the suspicious network is more with compare to proposed network.



(a)

(b)

Figure 6: UDP packet analysis; (a) in exiting system; (b) in proposed system.

V. CONCLUSION AND FUTURE SCOPE

Security in the mobile ad hoc network is very challenging task due the open communication and without centralized control. Proposed digital signature based technique gives good results as seen in the simulation results like give network throughput, minimize network load and give improved packet delivery ratio but as universal true that everywhere is an some area where the improvement are possible. Proposed framework is needed to test in the highly vulnerable environment such as attack like wormhole, black hole, DOS attack etc. in future different encryption algorithm will also combine with digital signature.

Proposed digital signature based technique gives good results as seen in the simulation results like give network throughput, minimize network load and give improved packet delivery ratio but as universal true that everywhere is an some area where the improvement are possible. Proposed framework is needed to test in the highly vulnerable environment such as attack like wormhole, black hole, DOS attack etc. in future different encryption algorithm will also combine with digital signature.

REFERENCES

[1] Jeenat Sultana; Tasnuva Ahmed2017 International Conference on Electrical, Computer and Communication Engineering (ECCE)Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems

[2] N Chaitanya Kumar; Abdul Basit; Priyadarshi Singh; V. Ch. Venkaiah2017 International Conference on Inventive Computing and Informatics (ICICI)

[3] Elbasher Elmahdi, Seong-Moo Yoo and Kumar Sharshembiev, 2018 securing data forwarding against black hole attacks in mobile Ad-hoc network.

[4] Amit Kumar Yogi; Jayesh Surana2016 International Conference on ICT in Business Industry & Government (ICTBIG)

[5] H.S. Chiu And K.S. Lui. DelPHI: Wormhole Detection Mechanism For Ad-Hoc Wireless Networks. In Proceedings International Symposium On Wireless Pervasive Computing, Phuket, Thailand, Jan. 2006.

[6] Ming-Yang Su. Warp: A Wormhole Avoidance Routing Protocol By Anamoly Detection In Mobile Ad-Hoc Networks. Computer Security, Vol.29, March 2010.

[7] F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, pp. 22-26, Apr, 2002.

[8] H.L.Nguyen,U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks," International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.

[9] H.Deng, W.Li and D.P.Agrawal, "Routing Security in Wireless Ad-Hoc Networks," University of Cincinnati, IEEE Communication Magzine, Oct, 2002.

[10] N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad-Hoc Network".

[11] V.Mahajan, M.Natue and A.Sethi, " Analysis of Wormhole Intrusion attacks in MANETs," IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[12] S. Kannan, T. Maragatham, Attack Detection and prevention methods in Proactive and Reactive Routing protocols, International Business Management 5(3), 2011

[13] Zhang, Lili, et al. "Group signature based privacy protection algorithm for mobile ad hoc network." Information and Automation (ICIA), IEEE International Conference on, 2017.

[14] Falgun Shah and Hitul Patel, "A Survey of Digital and Group Signature", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.6, June- 2016, pg. 274-278.

Authors Profile

Prof. Atul Dubey pursed Bachelor of Engineering from Jai Narayan college of Technology, Bhopal in 2010 and Master of Technology from All Saint's College of Engineeing Bhopal in year 2018. He is currently working as Assistant Professor in Department of Information Technology, Technocrats Institute of Technology, Bhopal since 20119. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 1 years of teaching experience and 1 years of Research Experience.