ANODR-ECC Key Management protocol with TELNET to secure Application and Network layer for Mobile Adhoc Networks

Dr.G.Padmavathi[1], Dr.P.Subashini[2], and Ms.D.Devi Aruna[3]
[1]Professor and Head, Department of Computer Science,
Avinashiligam University for Women, Coimbatore – 641 043
ganapathi.padmavathi@gmail.com
[2]Associate Professor, Department of Computer Science,
Avinashilingam University for Women, Coimbatore – 641 043
mail.p.subashini@gmail.com
[3]Project fellow, Department of Computer Science,
Avinashiligam University for Women, Coimbatore – 641 043
deviaruna2007@gmail.com

ABSTRACT

A mobile ad hoc network (MANETs) is a self-organizing network that consists of mobile nodes that are connected through wireless media. A number of unique features, such as lack of infrastructural or central administrative supports, dynamic network topologies, open communication channels, and limited device capabilities and bandwidths, have made secure, reliable and efficient routing operations in MANET a challenging task. The ultimate goal of the security solutions for MANET is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability to mobile users. To achieve the goals, the security solution need for entire protocol stack. . The proposed protocol ANODR-ECC with Telnet provide application layer security and it ensures route anonymity and location privacy and is robust against eavesdropping attack.For route anonymity, it prevents strong adversaries from tracing a packet flow back to its source or destination; for location privacy, it ensures that adversaries cannot discover the real identities of local transmitters. The simulation is done using network simulator qualnet 5.0 for different number of mobile nodes. The proposed model has exposed improved results in terms of Average throughput, Average end to end delay, Average packet delivery ratio and Average jitter.

KEYWORDS

MANET,Telnet ,ANODR-ECC, Evesdropping a ttack.

1. Introduction

A mobile ad hoc network (MANET) consists of mobile nodes without fixed infrastructure which are free to move at any speed in any direction and organize themselves randomly [6][8]. These nodes are constrained in power consumption, bandwidth, and computational power. MANETs are more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. They can also directly attacks the network inject false packets, or impersonate a node. This violates the network's goals of authentication, availability, integrity, and nonrepudiation 10][8]. Routing security is a paramount concern in MANETs and solutions to the routing security have been addressed in

DOI : 10.5121/ijdps.2012.3128

this paper. In which, anonymous routing is used for the purpose of security and privacy concerns. Anonymity protection in MANETs is one of the countermeasures against the mounting intrusions and attacks such as traffic analysis, spoofing, and denial of service. The proposed protocol provide application layer security and it ensures route anonymity and location privacy and is robust against eavesdropping attack .For route anonymity, it prevents strong adversaries from tracing a packet flow back to its source or destination; for location privacy, it ensures that adversaries cannot discover the real identities of local transmitters. The paper is organized in such a way that Chapter2 discusses proposed method, Chapter 3 discusses Experimental evaluation and Chapter 4 gives the conclusion

2. Proposed Method

This chapter briefly describes proposed method combines Anonymous On-Demand Routing-Elliptic Curve Cryptography (ANODR-ECC) and Telnet.

2.1. Anonymous On-demand Routing (ANODR) Protocol

ANODR is a reactive protocol. ANODR prevents strong adversary from packet flow back to its source or destination. For location privacy, ANODR ensures that adversaries cannot discover the real identities of local transmitters [2][3][5].

ANODR is realized upon a hybrid form of these two concepts.

- ANODR dissociates ad hoc routing from the design of network member's identity/pseudonym. An attacker can neither link network members' identities with their locations, nor follow a packet flow to its source and destination. Though the adversaries may detect the existence of local wireless transmissions, it is hard for them to infer a covert mission's number of participants, as well as the transmission pattern and motion pattern of these participants.
- ANODR has a special feature called intrusion tolerance**.** Node intrusion does not compromise location privacy of other legitimate members, and an on-demand ANODR route is traceable only if all forwarding nodes route are intruded ANODR provides the following security services:

a. Negligibility-based anti-tracing such that signal interceptors cannot trace signal transmitter's mobility pattern via wireless signal tracing (with non-negligible probability defined on the victim network's size).

b**.** Confidentiality and anonymity.

c. Traffic flow confidentiality.

d**.** Identity-free routing.

e. One-time packet contents such that any two wireless transmissions are indistinguishable with each other in regard to a cryptanalyst.

These services are provided at the Network Layer and Link Layer to protect the IP and link layer protocols.

2.2. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in ECC is an example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography. The mathematical operations of ECC is defined over the elliptic curve $\mathbf{y^2 = x^3 + ax + b}$**,**where $\mathbf{4a^3 + 27b^2 \neq 0}$. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA [6].

The proposed model combines Anonymous On-Demand Routing (ANODR) and Elliptic Curve Cryptography to provide node privacy, route anonymity and location privacy and is robust against wormhole attack than black attacks. For route anonymity, it prevents strong adversaries from tracing a packet flow back to its source or destination; for location privacy, it ensures that adversaries cannot discover the real identities of local transmitters[1][4].

2.3. Telnet

Telnet is a network protocol to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).Historically, Telnet provided access to a command-line interface on a remote host. The term *telnet* may also refer to the software that implements the client part of the protocol. Most network equipment and operating systems with a TCP/IP stack support a Telnet service for remote configuration. Telnet client applications are available for virtually all computer platforms. *telnet* means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface[9].

3. Experimentation and Evaluation

Qualnet5.0 network simulator is used for experimentation. Mobility scenarios are generated using a Random waypoint model by varying 10 to 50 nodes moving in a terrain area of 1500m x 1500m. The simulation parameters are summarized in Table 1

Parameter	**Value**
Simulator	Qualnet 5.0
Simulation time	100 s
Number of nodes	50
Traffic Model	CBR
Pause time	2 (s)
Maximum mobility	60 m/s
No. of sources	15
Terrain area	1500m x 1500m
Transmission Range	250m

The simulation is made to investigate the performance of the network's various parameters. The metrics used to evaluate the performance are:

1) Average packet delivery ratio

2) Average end-to-end delay

3) Average delay jitter

4) Average throughput

Average packet delivery ratio: The packet delivery ratio (PDR) of a receiver is defined as the ratio of the number of data packets actually received over the number of data packets transmitted by the senders. The average packet delivery ratio is the average of the packet delivery ratios taken over all the receivers.

Average End-to-End delay: The end-to-end delay of a packet is defined as the packet takes a time to travel from the source to the destination. The average end-to-end delay is the average of the end-to-end delays taken over all the received packets Eqn (1) is used to find the end to end delay of the packet.

$$delay = \frac{1}{nbx}\sum_{i\in x}\sum_{iey}\frac{delay_{j}}{nby} \quad \text{---- (1)}$$

x: is the set of destination nodes that received data packets.

nbx: is the number of receiver nodes

y: is the set of packets received by node i as the final destination.

Average delay jitter: Delay jitter is the variation (difference) of the inter-arrival times between the two successive packets received. Each receiver calculates the average per-source delay jitter from the received packets originated from the same source. The receiver then takes the average over all the sources to obtain the average per-receiver delay jitter. The average delay jitter is the average of the per-receiver delay jitters taken over all the receivers.

Average throughput: The throughput of a receiver (per-receiver throughput) is defined as the ratio over the time difference between the first and the last received packets. The average throughput is the average of the per-receiver throughputs taken over all the receivers. Eqn (2) is used to find the throughput of the packet.

$$Throuhput(\%) = \frac{\mathrm{Re}ceived \quad packets}{Sent \quad packets} * 100 \quad \text{---(2)}$$

Performance Comparison of ANODR-ECC with Telnet for Eavesdropping attack and Telnet.

The different parameters are considered for evaluation. Average packet delivery ratio, Average throughput, should be higher and Average end-to-end delay, Average delay jitter must be lower.

Figure 1shows that total byte received is higher in ANODR-ECC with Telnet for Eavesdropping attack and Telnet

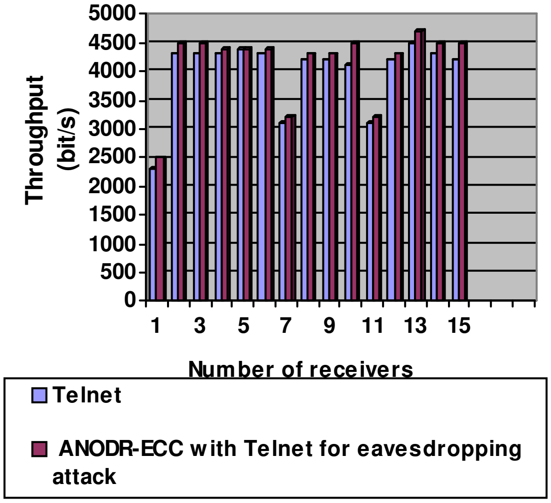

Figure1: Comparison of total bytes received of ANODR-ECC with Telnet for Eavesdropping attack and Telnet.

Figure 2 shows that throughput is higher in ANODR-ECC with Telnet for Eavesdropping attack and Telnet .

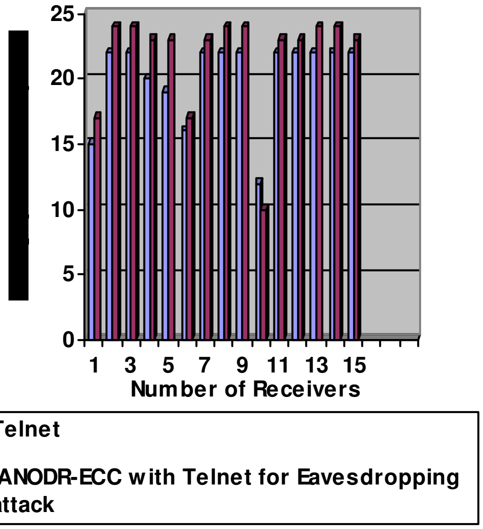

Figure 2: Comparison of throughput of ANODR-ECC with Telnet for Eavesdropping attack and Telnet.

Figure 3 shows that End-to-End Delay is lower in ANODR-ECC with Telnet for Eavesdropping attack and Telnet

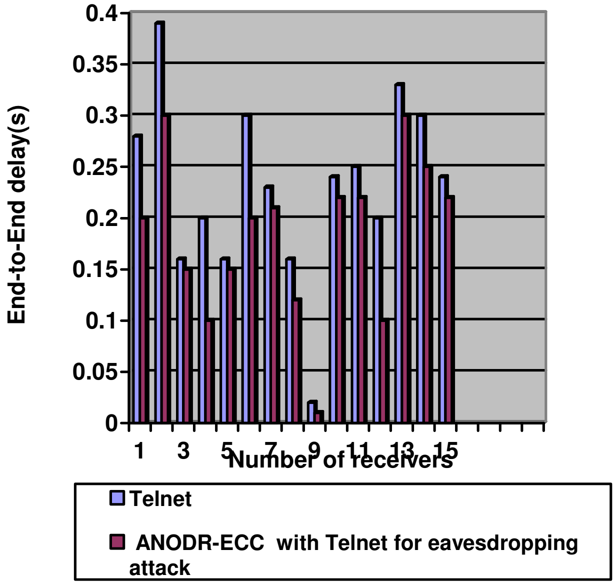

Figure 3: Comparison of End-to-End delay of ANODR-ECC with Telnet for Eavesdropping attack and Telnet.

Figure 4shows that jitter is lower in ANODR-ECC with Telnet for Eavesdropping attack and Telnet .

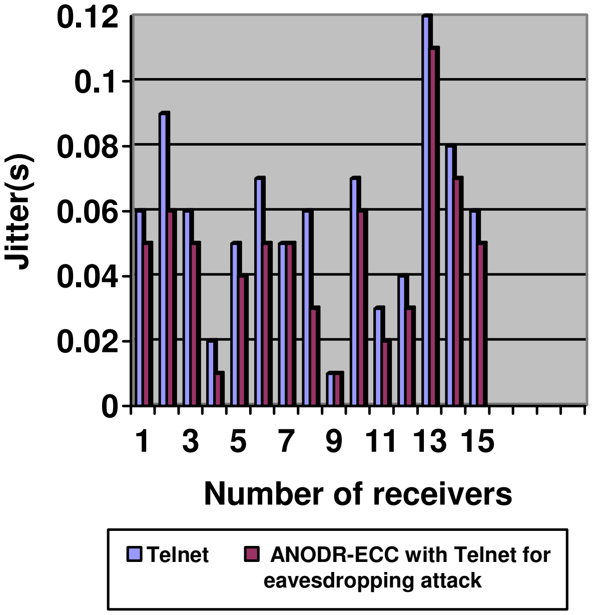

Figure 4 Comparison of jitter of ANODR-ECC with Telnet for Eavesdropping attack and Telnet .

4. CONCLUSION

A mobile ad hoc network (MANETs) is a collection of wireless mobile nodes dynamically forming a temporary network without any existing network infrastructure or centralized administration. Security and anonymity are important issues for mobile ad hoc network (MANETs) routing protocols. Particularly eavesdrop attacks are severe attacks against ad hoc routing protocols which is a challenging one to defend against. . The proposed protocol ANODR-ECC with Telnet provide application layer security and it ensures route anonymity and location privacy and is robust against eavesdrop attack .For route anonymity, it prevents strong adversaries from tracing a packet flow back to its source or destination; for location privacy, it ensures that adversaries cannot discover the real identities of local transmitters. The simulation is done using network simulator qualnet 5.0. The proposed model has exposed improved results in terms of Average throughput, Average end to end delay, Average packet delivery ratio, and Average jitter.

ACKNOWLEDGMENT

The authors would like to thank the University Grants Commission (UGC) for supporting this Major Research project (MRP).

References

1. L. C. Washington, ***Elliptic Curves: Number Theory and Cryptography***, Chapman & Hall/CRC, 2003

2. Jiejun Kong, Xiaoyan Hong, **"ANODR:** ***ANonymous On Demand Routing with Untraceable Routes for Mobile ad hoc Networks*"** *MobiHoc'03,* June 1–3, 2003

3. Papadimitratos, P. and Z. Haas. **"*Secure routing for mobile ad hoc networks*."** In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

4..G.V.S. Raju and R. Akbani, "***Elliptic Curve Cryptosystems and its Application****s*," in the proceedings of the IEEE-SMC Conference, October2003.

5..B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng, "***Anonymous secure routing in mobile ad-hoc networks***," in Proc. IEEE Intl. Conf. on Local Computer Networks, Tampa, USA, Nov. 2004.

6..Kristin Lauter, "***The Advantages of Elliptic Curve Cryptography for Wireless Security*"**, IEEE Wireless Communications, February 2004.

7. Latha Tamilselvan and V. Sankaranarayanan: "***Prevention of Black Hole Attack in MANET***", The 2nd international conference on wireless, Broadband and Ultra Wideband Communications (January 2007)

8.W. Wang, B. Bhargava, Y. Lu, and X. Wu, *"**Defending against wormhole attacks in mobile ad hoc networks***" *Wireless communication Mobile. Computing*, vol. 6, no. 4, pp. 483-503, June 2006.

9.N. G. Duffield, W. A. Massey, and W. Whitt. "**A nonstationary offered-load model for packet networks. Telecommunication Systems"**, 16(3-4):271–296, 2001.

10.L. Buttyan and J.-P. Hubaux, "**Security and Cooperation in Wireless Networks**," http://secowinet.epfl.ch/, 2006.

Dr. Padmavathi Ganapathi is the Professor and Head of Department of Computer Science, Avinashilingam University for Women, Coimbatore. She has 23 years of teaching experience and one year Industrial experience. Her areas of interest include Network security and Cryptography and real time communication. She has more than 110 publications at national and International level. She is a life member of many professional organizations like CSI, ISTE, AACE, WSEAS, ISCA, and UWA.

Dr. Subashini is the Associate professor in Department of Computer Science, Avinashilingam Deemed University for Women, Coimbatore. She has 18 years of teaching experience. Her areas of interest include Object oriented technology, Data mining, Image processing, Pattern recognition. She has 95 publications at national and International level**.**

Ms.D.Devi Aruna. received MCA Degree from Avinashilingam University for Women, Coimbatore in 2008 respectively and pursuing her Ph.D in same University. She is currently working as a Project Fellow in UGC project in Department of Computer Science in the same University and has three year of research experience. Her research interests are cryptography and Network Security. She has 12 publications at national and international level.