ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

An Efficient Dynamic Authenticated Secure Routing Using Secure Elliptic Curve Cryptography in MANET

V.Deepadharsini[1], VR. NAGARAJAN[2]

M.Phil Research Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore, India[1]

Assistant Professor, Department of Computer Science, Sree Narayana Guru College, Coimbatore, India[2]

ABSTRACT: A wireless network consists of two or more mobile nodes that are linked in order to share resources, exchange files, or allow message communications. MANET protocols have to face high challenges due to dynamically changing of topologies, low transmission power and asymmetric links. To address the core issue of data routing protocol, in this paper proposed a Dynamic Authenticated secure routing (DASR) using encryption scheme combines the advantages of proactive and reactive routing. The objective of this paper is designed, implemented and evaluated a multi-hop ad hoc network using Dynamic Authenticated secure routing (DASR) algorithm with Secure Elliptic Curve Cryptography in NS 2.34 Framework. Each secure routing path communicates wirelessly with another using the IEEE 802.11b technology without any aid of infrastructure. The main protocol implemented in this application was the DASR algorithm, which consists of two important mechanisms, Multipoint Transmit (MPT) and shortest path routing.

KEYWORDS: MANET; secure routing; elliptic curve cryptography; MPT

I. INTRODUCTION

Mobile ad hoc networks (MANETs) enclose have been an important group of networks, provided that message support in assignment significant scenarios including battlefield and strategic assignments, find and save operations, and tragedy release operations. Cluster infrastructure has been necessary for huge applications in MANETs. The characteristic number of users of MANETs has always increased, and the applications carried by these systems have become increasingly resource demanding. In this turn, has increased the significance of bandwidth effectiveness in MANETs. It is essential for the medium access control (MAC) protocol of a MANET not only to adjust to the dynamic environment but also to efficiently manage bandwidth consumption.

Self-configurable characteristic and arbitrary topology of the MANET fulfill the requirements of such systems where it requires a real-time data exchange and processing without being concerned with the geographical changes in the topology. Even though MANET is considered as a robust and scalable network infrastructure, it undoubtedly prompts numerous concerns in several areas such as security, availability, reliability and resilience. MANET is definitely a crucial research topic and it requires a completely different approach of analysis than the already known wired networks.

In the security aspect, MANET has different personality and characteristics that surely trigger their own specific security concerns. Since MANET has high mobility, no administrative node to control the network and open network. Every node can participate in the network easily makes MANET more vulnerable to an adversary's malicious attacks. Many potential attacks can be performed in each communication layers. MANET is more prone to physical threats than wired networks and it promotes an environment for several attacks such as spoofing, eavesdropping and Denial of Service (DoS) attacks. Most of these attacks are directed to the routing protocol schemes and they tamper some of their activities taking advantage of their insecure implementation and architecture.

Under these constraints, the routing protocol challenge in MANET is how to develop a robust security aware routing protocol that will eliminate the attacks existing in MANET without consuming the overall performance. In this dissertation we propose a solution for routing protocol to cover the performance and security problem in MANET.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

II. RELATED WORK

In [1] authors discussed the secure transmission of information in wireless networks without knowledge of eavesdropper channels or locations is considered. Two key mechanisms are employed: artificial noise generation from system nodes other than the transmitter and receiver, and a form of multi-user diversity that allows message reception in the presence of the artificial noise. To determine the maximum number of independently-operating and uniformly distributed eavesdroppers that can be present while the desired secrecy is achieved with high probability in the limit of a large number of system nodes. In [2] proposed the effectiveness and straight forward implementation of physical layer jammers make them an essential security threat for wireless networks. In [3] authors discussed the information theoretic security has recently emerged as an effective physical layer approach to provide secure communications. Provide that the legitimate receiver and eavesdropper have the same noise power, many existing secure schemes cannot achieve outage probability approaching zero, regardless of how large the transmission power is. In [4] Authors framework illustrates the dependence of the network throughput on key system parameters, such as the densities of legitimate nodes and eavesdroppers, as well as the QoS and security constraints. One important finding is that the throughput cost of achieving a moderate level of security is quite low, while throughput must be significantly sacrificed to realize a highly secure network. In [5] authors suggested as a multi-hop wireless network and a source destination pair of nodes to addressed the problem of jointly selecting a communication route and allocating transmit power levels, so that the end-to-end spectral efficiency of the route exceeds a desired threshold. The transmit power level, however, has been assumed to be known, and route selection was considered in isolation. In [6] authors studied the cooperative transmission for securing a decode-and-forward (DF) two-hop network where multiple cooperative nodes coexist with a potential eavesdropper. Under the more practical assumption that only the channel distribution information (CDI) of the eavesdropper is known, they proposed an opportunistic relaying with artificial jamming secrecy scheme, where a "best" cooperative node is chosen among a collection of N possible candidates to forward the confidential signal and the others send jamming signals to confuse the eavesdroppers. In [7] authors considered a cooperative wireless network in the presence of one or more eavesdroppers, and exploit node cooperation for achieving physical (PHY) layer based security. Two different cooperation schemes are considered. In the first scheme, cooperating nodes retransmit a weighted version of the source signal in a decode-and-forward (DF) fashion.

III. PROPOSED ALGORITHM

The proposed architecture accepts the simulation parameters as input which contains the NS2.34 simulation where the novel secure distributed map detection algorithm is applied to the mobile ado network. This overall proposed architecture.

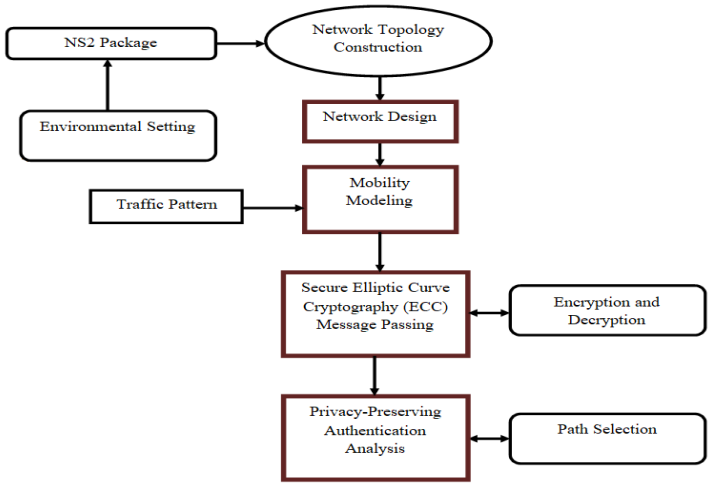

Fig. 1: Proposed Architecture

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

A. *Network Model*

The network model in this section concerning the Distributed Path Vector (DPV) protocol is taken from its AODV routing. It is a proactive routing protocol, so the routes are always immediately available when needed. DPV is an optimization version of a pure link state protocol. So the topological changes cause the flooding of the topological information to all available hosts in the network. To reduce the possible overhead in the network protocol uses Multipoint Relays (MPR). The idea of MPR is to reduce flooding of broadcasts by reducing the same broadcast public encryption keys in some regions in the network,

B. *Mobility Modeling*

The random waypoint model (RWP) is one of the most widely used mobility models in performance analysis of ad hoc networks. This model analyse the stationary spatial distribution of a node moving according to the RWP model in a given convex area. For this it gives an explicit expression, which is in the form of a one-dimensional integral giving the density up to normalization constant. This result is also generalized to the case where the waypoints have a non-uniform distribution.

C. *Secure Elliptic Curve Cryptography (ECC) Message Passing*

The Secure Elliptic Curve Cryptography (ECC) process nodes receive messages from the entire network. If there is any traffic jam situations occurring in the networks, the nearby neighbour nodes informs the destination. The mobile nodes broadcast this alert message to other nodes in the network. So that other nodes may take an alternative route or take some other decision regarding the issue. Message sending and receiving will be strongly encrypted using elliptic curve cryptography algorithm. Thus only encrypted data will be passed and retrieved from the source node. Elliptic Curve Cryptography (ECC) will be used for secure transactions for message communication which might ensure its security for changes.

Algorithm 1: Elliptic Curve Encryption
Input: Parameters from the elliptic curve domain (p, E, P, n), Public Key Q, Message m
Output: Encrypted text (C1, C2) begin
Step 1: Represent the message m as a point M in E(Fp)
Step 2: Select k ∈ R[1,n−1].
Step 3: Calculate C1 = kP
Step 4: Calculate C2 = M + kQ.
Step 5: Return (C1, C2)

Algorithm 2: Elliptic Curve Decryption
Input: Parameters from the elliptic curve domain (p, E, P, n), Private key d, Encrypted text (C1, C2)
Output: Message m begin
Step 1: Calculate M = C2- dC1 and extract m from M.
Step 2: Return (m).

The message *m* is firstly represented as a point M and then it is encrypted by adding *kQ*, where *k* is a randomly chosen integer and *Q* is the public key. The broadcaster transmits the points *C1* = *kP* *eC2* and *eC2* = *M* + *kQ* to the receiver, which uses its private key to calculate *dC1* = *d*(*kP*) = *k*(*dP*) = *kQ* and then compute *M* = *C2* − *kQ*. An intruder who wishes to read M needs to calculate *kQ*.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

D. *Dynamic Authenticated Secure Routing (DASR)Process*

The Secure encryption process nodes receive messages from the entire network. If there is any traffic jam situations occurring in the networks, the nearby neighbor nodes informs the destination. The mobile nodes broadcast this alert message to other nodes in the network. Message sending and receiving will be strongly encrypted using encryption algorithm. Thus only encrypted data will be passed and retrieved from the source node. It predicts the distributed attacks (jammers) in mobile adhoc network.

The efficiency of this ECC algorithm is based on finding a discrete logarithm of a random element, which belongs to an elliptic curve. In order to get an idea of the applicability of elliptic curves-based algorithms, in devices with computational restrictions that the efficiency of the ECC encryption algorithm, with keys to approximately 160 bits, is the same obtained from the 1024-bit key. Algorithms from several functionalities are based on elliptic curves, including key management, encryption and digital signature. The main idea of this algorithm is to construct a set of points of an elliptic curve in that the logarithm problem is unapproachable. According to cryptographic systems based on elliptic curves reach the same security level security systems, utilizing smaller keys, hence consuming less memory resources and processor

IV. SIMULATION RESULTS

The simulation studies involve the deterministic large network topology with 50 to 100 nodes. The proposed Dynamic Authenticated secure routing (DASR) algorithm is implemented with MATLAB R2010a. The DASR algorithm is compared with existing Static Authenticated Secure Routing (SASR) method with throughout metrics ratio.

Throughput: The ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet is referred to as throughput. It is expressed in bits per second or packets per second. Factors that affect throughput include frequent topology changes, unreliable communication, limited bandwidth and limited energy.

$$\boldsymbol{EX} = \frac{\boldsymbol{C}}{\boldsymbol{T}} \quad eqn.\,(1)$$

Where X is the throughput, C is the number of requests that are accomplished by the system, and T denotes the total time of system observation.

Table 1: Comparison of Throughput measures of Existing SARS and Proposed DARS algorithm

Methods	**10**	**20**	**30**	**40**	**50**
SARS	10	20	45	80	85
DASR	**10**	**35**	**65**	**86**	**92**

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

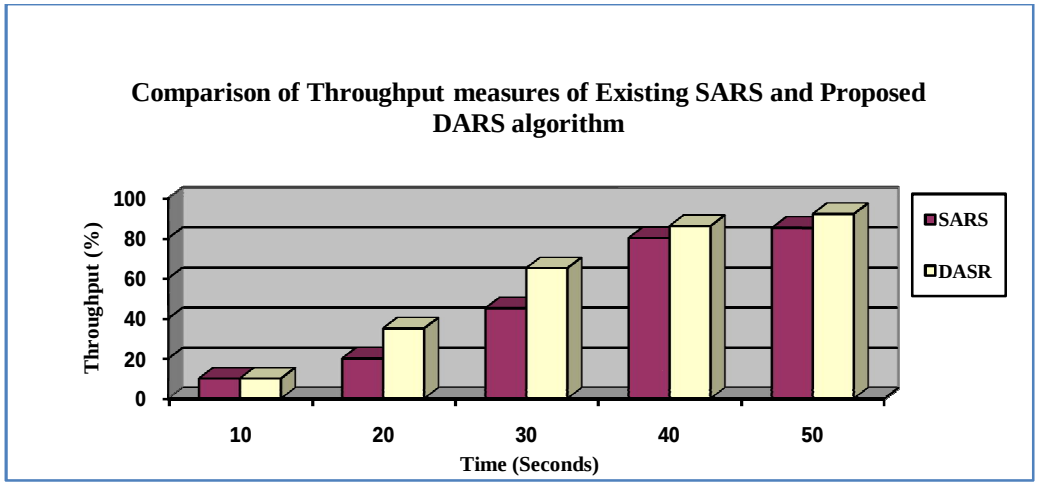

Fig. 2: Comparison of Throughput measures

V. CONCLUSION AND FUTURE WORK

In this paper presents a new approach which combines techniques from various fields and adapts to solve the problem of secure routing, shortest path selection and packet detection accuracy. The goal of this research is designed, implemented and evaluated a multi-hop ad hoc network using Dynamic Authenticated secure routing (DASR) algorithm with Secure Elliptic Curve Cryptography in NS 2.34 Framework. Each secure routing path communicates wirelessly with another using the IEEE 802.11b technology without any aid of infrastructure. The main protocol implemented in this application was the DASR algorithm, which consists of two important mechanisms, Multipoint Transmit (MPT) and shortest path routing.

REFERENCES

1. D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," IEEE J. Sel. Areas Commun., vol. 29, no. 10, pp. 2067–2076, Dec. 2011.
2. A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Jamming-aware minimum energy routing in wireless networks," in Proc. IEEE Int. Conf. Commun. (ICC), June 2014, pp. 2313–2318.
3. Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," IEEE J. Sel. Areas Commun., vol. 30, no. 2, pp. 359–368, Feb. 2012.
4. X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," IEEE Trans. Wireless Commun., vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
5. M. Saad, "Joint optimal routing and power allocation for spectral efficiency in multi-hop wireless networks," IEEE Trans. Wireless Commun., vol. 13, no. 5, pp. 2530–2539, May 2014.
6. C. Wang, H.-M.Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," IEEE Trans. Wireless Commun., vol. 14, no. 2, pp. 589–605, Feb 2015.
7. J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," IEEE Trans. Signal Process., vol. 59, no. 10, pp. 4985–4997, Oct. 2011.