ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(19), DOI: 10.17485/ijst/2016/v9i19/86081, May 2016* ISSN (Online) : 0974-5645

Unreliable Node Detection by Elliptical Curve Diffe-Hellman Algorithm in MANET

S. John Justin Thangaraj[1*] and A. Rengarajan[2]

[1]Department of Computer Science and Engineering, St. Peter's University, Chennai - 600 054, Tamil Nadu, India
[2]Department of Computer Science and Engineering, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai - 600062, Tamil Nadu, India

Abstract

Objective: The purpose of this scheme is to detect unreliable node from routing and provide reliable data transmission in MANET. **Method:** The openness in network topology and deficiency of the central administration leads to vulnerable attack in MANET. In order to decrease the threat in Mobile Ad-hoc Network (MANET), we propose Unreliable node Detection by Elliptical Curve Diffe-Hellman in MANET (UD-ECDH). **Findings:** The UD-ECDH scheme exchanges the secret key to detect the unreliable node and isolate from routing thus increasing the network performance. **Improvement:** The simulation results show that this scheme assure better packet delivery, improve throughput, reduces the delay and energy consumption in the network.

Keywords: Elliptical Curve Diffe-Hellman Algorithm, Energy, MANET, Reliability

1. Introduction

A MANET is a self-organized multi-hop system comprised by multiple mobile nodes with peer-to-peer relationship. MANET does not have any preset structure and contains number of nodes that movement vigorously not including any margin limitations. Advantages are rapid to install, grant fault tolerance, connectivity and mobility. However, the MANET's challenges are dynamic topology, open medium, bandwidth constrained; link capacity, energy-constrained operation and inadequate physical refuge. The lack of central administration and unreliable wireless link, vulnerability, security threats leads to improve security in MANET. Without security the intruder, easily attack the network during data transmission. It habitually endures from attacks by selfish or malevolent nodes. For example on-off attack, grey hole attack, bad mouthing attack, inconsistency behavior attack, black hole attack, wormhole attack and so on[1].

To solve the above problem we apply an Elliptic curve cryptography and Diffie-Hellman key exchange algorithm that provides secrecy for web browser application using HTTPS. It provides protection against man in the middle attacks and bidirectional encryption communications between client and server that grant security against eavesdropping and tampering and establish the contents of the communications. This algorithm present faster calculations and conserve the energy, memory and bandwidth. In this paper, we propose Elliptical Curve Diffie-Hellman Algorithm based on un-reliable node detection in MANET. ECDH algorithm provides the security against the unreliable node insecure wireless channel.

Key agreement protocol was used in communication and true relay participation in the public exchange. Tradeoff between security and protocol effectiveness is measured in the join design of benefit refinement, privacy amplification as well as information resolution[2]. This method achieve secret key rate while an opponent has more positive channel conditions. Random seed distribution assumes the random allocation of secret matter as well as transitory master key is utilized to create a pair-wise key[3]. Hop-by-Hop Authentication scheme was based on Elliptical Curve Cryptography

* *Author for correspondence*

(ECC) that provides mediate hop verification and source privacy[4]. This scheme reduces the computational and communication overhead.

Ring-based reliable multicast routing technique is reliable and robust against link failures in MANETs[5]. Convex Hull algorithm was used to discover the external edge of the system and to generate a consistent ring. This scheme works efficiently to progress the performance of path establishment and path finding overhead for different movement environment. Exponential Reliability Coefficient based reputation Mechanism (ERCRM) isolates the selfish node from the routing path based on Exponential Reliability Coefficient (EXRC)[6]. This reliability coefficient manipulated during the exponential failure rate was based on moving average method that highlights the average path behavior of the mobile nodes for quantifying its realness. Fuzzy Based Intrusion Detection Systems to identify the malevolent behavior of node by intrusion detection also identify the type of attacks[7]. This technique detects and prevents the gray hole and black hole attacks in the network.

Distributed detection scheme detects the malevolent node rapidly, and that a mobile malevolent node can only avoid discovery for a very restricted period[8]. Detection of Malevolent Nodes (DMN) effectively detects malevolent nodes that drop and replica packets in the network and therefore develop the performance of the system[9]. Game theoretic approach detects the malicious node and improves the network throughput[10]. The trust management scheme gives an indication about trust routing[11]. It utilizes trust values to favor packet sending by maintenance a trust counter for each node. But, the trust counter value decrease less than threshold, that node is distinct as malevolent and inaccessible from the network. However, the energy consumption is high. Fuzzy Trusted Dynamic Source Routing (FTDSR) protocol evaluates the effectiveness of the protocol in identifying malevolent also provides attack resistance[12]. However, this technique does not detect the dynamic behavior of the node. Communication based detects the selfish nodes based on the energy level and Node Communication Ratio (NCR). This scheme has improved quality of service[13].

Energy based AODV (E-AODV) that assures the protection of privacy, honesty and accessibility triangle[14]. Privacy is provided by computing Intermediate Trust Value (ITV) for all nodes among sender and receiver. The highest ITV nodes are used for data transmission. The digital signature algorithm provides data integrity. Availability has been provided by computing the remaining energy of every node. In this scheme, the highest remaining energy node is selected for data transmission.

The paper is structured as follows. Section 2 describes Elliptical Curve Diffie Hellman (ECDH) algorithm to detect the unreliable node. Section 3 describes the results and discussion for evaluating the efficiency of the proposed method. Lastly, section 4 concludes the paper.

2. Proposed Method

A Reliable Route Selection Scheme (RRSS) estimates the node's arrival angle using RSS variations to obtain route's lifetime and to decision about the convenience of an adjacent node[15]. However, this method does not detect the unreliable node in MANET. To overcome this problem, a novel reactive routing protocol is proposed that detects the unreliable node in MANET.

Unreliable node may loss the packet or modifies the packet during data transmission. Elliptical Curve Diffie Hellman (ECDH) algorithm was designed to maintain and provide reliability in MANET. ECDH algorithm detects the unreliable node from participating in the routing operation. In this scheme, key exchange using ECDH is done by the following steps.

The simple Weierstrass equation is given in (1)

$$y^2 = x^3 + ax + b \tag{1}$$

$E_q(a,b)$ Elliptic curve with parameters a, b and q

Where q is a prime integer of the form 2^m

Every node is assigned the private key and this key is kept in secret. The private key is estimated in (2).

$$\Pr = \sum_{i=0}^{k} n_i$$

Where $n_i < n$ (2)

The source broadcasts RREQ message to its adjacent nodes. RREQ message contains source node id, receiver id and source public key. The public key is calculated by (3).

$$Pu = \sum_{i=0}^{k} n_i * \gamma$$

Where $n_i < n$ (3)

Where γ is a point on elliptic curve whose order is large value n

Every node that obtains the broadcast, examines the destination to notice if it is deliberate recipient. If sure, it sends a Route Reply (RREP) message back to the source. RREP message contains destination secret key. The secret key is estimated by (4).

$$K_s = \sum_{i=0}^{k} \Pr * Pu \quad (4)$$

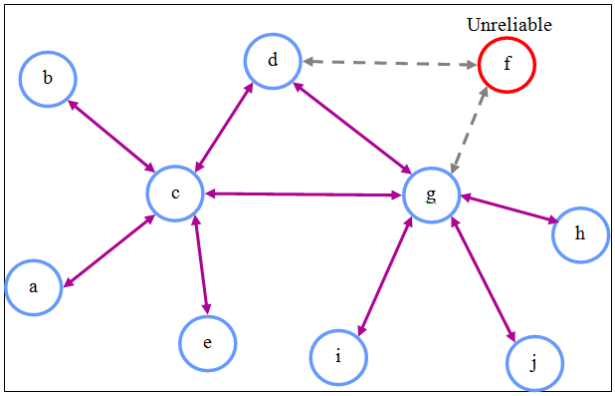

Figure 1. ECDH key verification among nodes.

All nodes are verified using the ECDH key verification process. If the node passes the verification then transmit the data to the verified node. If the node detects the unreliable, then broadcast the information to all nodes and remove that node from the routing.

Figure 1 shows the ECDH Key verification among nodes in the network. The secret key of source and all nodes is equal, but the secret key of node *f* and secret key of source is not equal. Therefore, the source send notification message to all nodes. All nodes therefore recognize *f* as an unreliable node and avoid the data transmission to this node.

Algorithm

1. Input Source S, Receiver R, Intermediate node N
2. Output Reliable forwarder node
3. Begin Procedure
4. While S not reaches the R do
5. Collect N neighbors
6. Foreach neighbor do
7. Check secret key
8. If (SKs = SKi)
9. N is a reliable node
10. Choose N is a forward node goto (4)
11. Else
12. Broadcast N is an unreliable node
13. Source select next near node N goto (4)
14. End Procedure

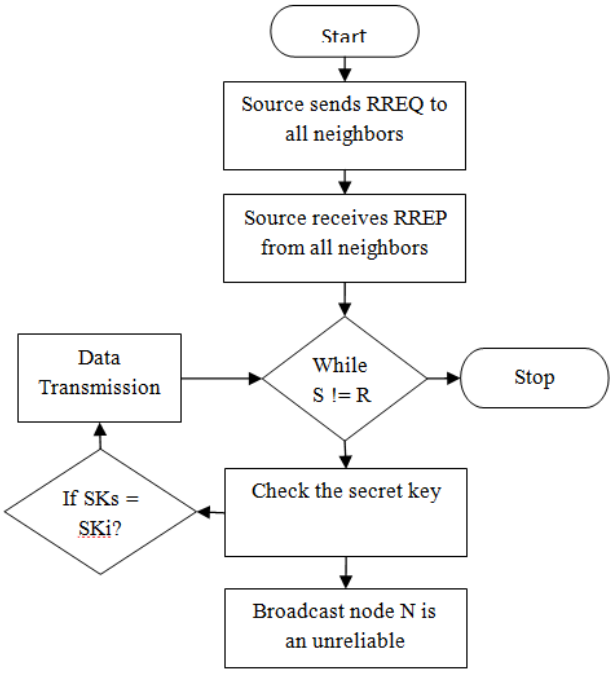

Figure 2. UD-ECDH scheme.

Figure 2 shows the flowchart of the Unreliable node Detection scheme using Elliptical Curve Diffe-Hellman Algorithm. Primarily the source sends Route Request (RREQ) message to all its neighbor nodes. Then source receives the RREP message from the neighbor node and the source checks the secret key of every node. If the key matches, then the source send the data, else the source sends notification message to all nodes that the corresponding node is an unreliable one.

3. Results and Discussion

The performance evaluation is observed using the network simulator, which is generally used by most researchers especially for simulation of wireless networks. The simulation parameters used for the communication strategies are tabulated in Table 1. The network performance metrics like packet delivery, packet loss, throughput and energy are compared against the existing system to get the percentage improvement by using EFSM in WSN.

Table 1. Simulation parameters

Simulation Parameter	Value
Simulation area	800×800m
Number of nodes	50
Simulation Time	50 ms
Initial Energy	1 J
Communication protocol	User Datagram Protocol (UDP)
Traffic Model	Constant Bit Rate (CBR)
Propagation model	Two ray ground
Antenna Type	Omni Antenna
MAC type	IEEE 802.11
Mobility Model	Random way point

3.1 Packet Delivery Rate

The Packet Delivery Rate (PDR) is the rate of the total packets received over the simulation time in the WSN considered. The PDR is calculated by (5).

$$PDR = \frac{Total\ Packets\ Received}{Total\ Packets\ Send} \quad 5)$$

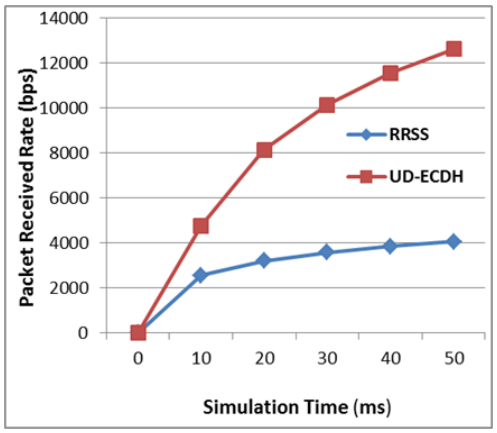

Figure 3. Packet delivery rate.

The PDR of UD-ECDH and RRSS protocol are shown in Figure 3. The PDR of the proposed UC-ECDH is greater than the PDR of the existing RRSS scheme.

3.2 Packet Loss Rate

The number of packets dropped during data transmissions in the simulation time considered is measured as the Packet Loss Rate (PLR). The numbers of packets lost while operating with both mechanisms are shown in Figure 4.

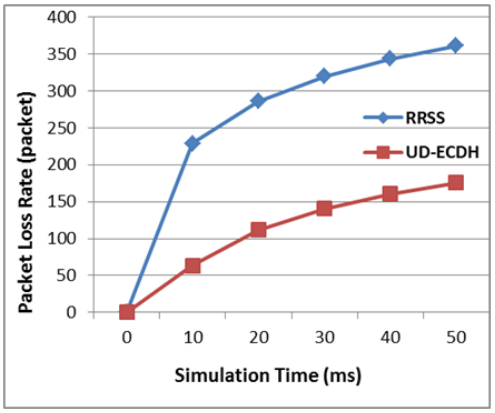

Figure 4. Packet loss rate.

$$PLR = \frac{Total\ Packets\ Dropped}{Total\ Packets\ Send} \quad (6)$$

The PLR is estimated in (6). PLR of the UD-ECDH is lower than the RRSS in Figure 4. Lower packet loss represents the better operation of the network.

3.3 Average Delay

The average delay is defined as the time difference between the each packet send and received at any instance of time. It is measured by (7).

$$Avg\ Delay = \frac{\sum_{0}^{n} Pkt\ Send\ Time - Pkt\ Recvd\ Time}{Time} \quad (7)$$

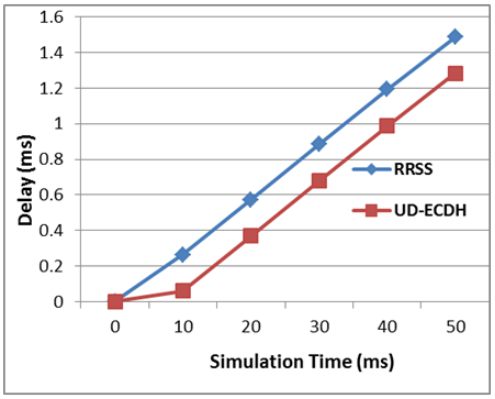

Figure 5. Average delay.

Figure 5 indicates that the delay value is low for the UD-ECDH than the existing scheme RRSS.

3.4 Throughput

It is one of the most essential parameters for routing in the network. Figure 6 shows the throughput at various time intervals for both RRSS and UD-ECDH protocols. Throughput is estimated by (8).

$$Throughput = \frac{\sum_{0}^{n} Pkts\,Received(n) * Pkt\,Size}{1000} \quad (8)$$

It can be observed from Figure 6 that the throughput is increased in the proposed method than the existing method.

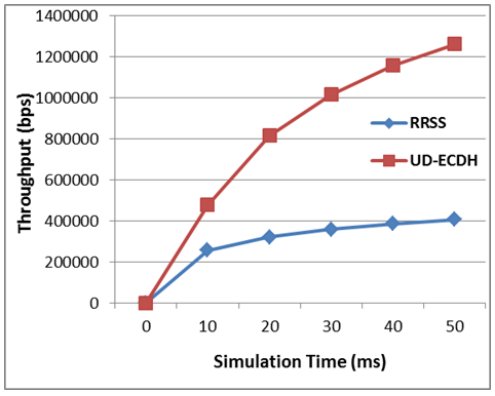

Figure 6. Throughput.

3.5 Residual Energy

A measure of the residual energy gives the rate at which energy is consumed by the network operations. Energy consumption is the typical amount of energy used up by all the nodes in the network. The initial energy of the nodes is 1J and for every operation, there is a regular reduction of energy for every node.

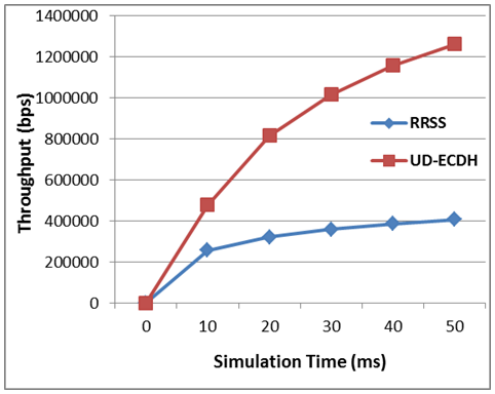

Figure 7. Residual energy.

The difference between the average energy consumption of the RRSS protocol and the UD-ECDH protocols are shown in Figure 7.

4. Conclusion

In this paper, we proposed Unreliable node detection by Elliptical Curve Diffe-Hellman Algorithm in MANET. This scheme detects the unreliable node and provides reliable data transmission in network. The unreliable node is detected based on ECDH's secret key. Therefore, it provides better reliability and extends the network performance when comparing to the existing RRSS scheme. Our simulation results demonstrate that this scheme provides guaranteed packet delivery rate, improves the throughput, reduces the delay and energy consumption in MANET.

5. References

1. Sun, YL, Han Z, Yu W, Ray LKJ. Attacks on trust valuation in distributed networks. Proceedings of 40th Annual Conference on Information Sciences and Systems; 2006 Mar. p. 1461–6.
2. Wang N, Zhang N, Gulliver TA. Cooperative key agreement for wireless networking: Key rates and practical protocol design. IEEE Transactions on Information Forensics and Security. 2014; 9(2):272-84.
3. Gandino F, Montrucchio B, Rebaudengo M. Key management for static wireless sensor networks with node adding. IEEE Transactions on Industrial Informatics. 2014; 10(2):1133-43.
4. Ian L, Yun L, Ren J, Wu J. Hop-by-hop message authentication and source privacy in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2014 May; 25(5).
5. Biradar RC, Manvi SS. Agent-driven backbone ring-based reliable multicast routing in mobile ad hoc networks. IET Communications. 2011 Jan; 5(2):172-89.
6. Sengathir J, Manoharan R. Exponential reliability coefficient based reputation mechanism for isolating selfish nodes in MANETs. Egyptian Informatics Journal. 2015; 16(2):231–41.
7. Balan EV, Priyan MK, Gokulnath C, Devi GU. Fuzzy based intrusion detection systems in MANET. 2nd International Symposium on Big Data and Cloud Computing; 2015. p. 109–14.
8. Jun-Won H, Matthew W, Das SK. Distributed detection of mobile malicious node attacks in wireless sensor networks. Ad Hoc Networks. 2012; 10:512–23.
9. Khan U, Agrawal S, Silakari S. Detection of Malicious Nodes (DMN) in vehicular ad-hoc networks. Procedia Computer Science. 2015; 46:965-72.

10. Wang W, Chatterjee M, Kwiat K, Li Q. A game theoretic approach to detect and co-exist with malicious nodes in wireless networks. Computer Networks. 2014; 71:63-83.
11. Aravindh S, Vinoth RS, Vijayan RA. Trust based approach for detection and isolation of malicious nodes in MANET. International Journal of Engineering and Technology. 2013 Feb-Mar; 5(1).
12. Xia H, Jia Z, Ju L, Zhu Y. Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory. IET Wireless Sensor System. 2011; 1(4):248–66.
13. Kumari DS, Sikamani KT. Communication based clustering to detect selfish nodes in MANET. Indian Journal of Science and Technology. 2015; 8(20).
14. Sumathi A, Sundaram VB. An ANN approach in ensuring CIA triangle using energy based secured protocol E-AODV for enhancing the performance in MANETS. Indian Journal of Science and Technology. 2015; 8(34).
15. Reina DG, Tora SL, Jonhson P, Barrero F. A reliable route selection scheme based on caution zone and nodes' arrival angle. IEEE Communications Letters. 2011; 15(11).