Cluster Computing (2019) 22:S4017–S4025
https://doi.org/10.1007/s10586-018-2612-2

A curve based cryptography for wireless security in MANET

N. Sridevi[1] · V. Nagarajan[1]

Received: 27 February 2018 / Revised: 15 March 2018 / Accepted: 18 March 2018 / Published online: 29 March 2018

Abstract

Mobile Ad hoc Network (MANET) is a mobile and infrastructure less network, widely used in various applications. In this paper, we study the major security issues in MANET to reduce the malicious activity at the nodes. To reduce the unsecured network, Enhanced Adaptive Acknowledgement Scheme (EAACK) is proposed and it involves Acknowledgement (ACK), Secure Acknowledgement (SACK), and Misbehavior Report Authentication (MRA) schemes. In EAACK scheme, the 2b (2-Bit) packet header is used and it overcomes some of the disadvantages of Watchdog behavior. In this work, the sender has to digitally sign the ACK packets and the receiver has to verify it. The proposed Scheme is applied to 40% of malicious nodes and Routing overhead (Ro) hits the value 0.6. The Network performance is better when the value of Ro is 0. In order to secure more, Credibility Based Sequence Distance Vector Routing (CBSDV) and Curve based cryptographic technique is used. Simulation results show that proposed scheme provides better secure network and CBSDV, hop count, time duration, energy values and trust scores play a deciding factor between the source and destination in the network.

Keywords Credibility based sequence distance vector routing · Curve based cryptography · Enhance adaptive acknowledgement · Acknowledgement · Secure acknowledgement · Misbehaviour report authentication · Mobile ad hoc networks

1 Introduction

Nowadays, due to advancement in technology in the area of wireless networks there are security threat issues, especially, malicious entry to the nodes. It is mandatory to protect the data and resources from security attacks and safeguard the network. In areas of applications like military, rescue operations, government, business and academic organizations, eavesdropping and electronic fraud are major risks to the administration. When some secret information has to be shared between two parties, messages should be encrypted using strong algorithmic concepts, digitally signed and properly authenticated. Proper selection of routing protocols and hashing functions play a major role in network security. In MANET, the secure, efficient distance vector routing for MANET (SEAD) [1] described the evaluation of dynamic sequence distance vector (DSDV) for the secure routing protocol. This process supports the protection to denial of Service (DOS) attacks and robust compared to a couple of encoding attackers rising the incorrect routing state in a few other nodes. According to this, SEAD shared has to be more readily authenticated. The enhanced acknowledgement concept has been proposed [2] in which the malicious nodes are detected with the help of the techniques such as acknowledgement (ACK), SACK, and MRA.

Considering the ACK, the sender sends a message to the receiver through a direction by the help of a signed keying technique. This technique uses a separate hash function called hand key function ‘S’. The signed messages are sent to the receiver through intermediate nodes to the destination and destination node after receiving a message, it sends back the ACK message back to the sender node. If the ACK message is received in a particular time, then the network is said to be good. If the ACK message is not received, then the algorithm moves to next phase SACK. In a SACK, the root nodes are clustered and ACK messages are sent in-between them, if some of the nodes are not

✉ N. Sridevi
86sridevi86@gmail.com; sakthisri86@gmail.com

V. Nagarajan
nagarajan.velmurugan.dr@ieee.org

[1] Department of ECE, Adhiparasakthi Engineering College, Melmaruvathur, India

sending the ACK message then the node is detected as malicious node and the report is sent to sender for verification.

During verification, the sender node receives the report packets, and reverts those particular packets to the destination in alternate path. The receiver checks for correctness and the destination's report is matched with the sender's report after which the node is marked as malicious node. But they still lack the ability to efficiently classify the normal node from the malicious node. The hybrid approach of efficient Intrusion Detection System [3] has been proposed to identify isolation of attacks by using reactive and proactive protocols. Here a cluster forms and chooses a cluster head to transfer the packets among other nodes without malicious activities. But the rule for cluster consistency has to be improved in fuzzy control systems. A fuzzy based system has been proposed [4] by comparing the cluster nodes to improve security.

But this paper spends a lots of time and energy for detecting the malicious via locally and globally by broadcasting the key. Fuzzy based application has been proposed [5–8] to improve the security of cluster nodes as well as system performance by selecting the nodes with a secret key. Schemes such as F2SMC2 and F2SMC1 have been introduced. The F2SMC2 is more complex while analyzing this concept. Uncertainty Analysis Framework (UAF) has been proposed to calculate network belief, disbelief, and uncertainty (BDU) values, in which the network belief and gain increase in Packet delivery ratio to improve more trust, based routing protocol. According to this paper there are no sophisticated parameters to measure, disbelief and uncertainty values.

An optimized Fingerprint Minutiae-point Non-invertible Key (FMNK) [9–11] has been proposed to secure, authenticates the MANET by using a Secure Socket Layer (SSL) as well as utilizing a biometric image model. Here the information is encrypted by applying key to increase security. By rendering this concept and using SSL encryption algorithm m model with FMK key produces more complexity. As we observe from the literature that most of the investigations still require more security and less complexity. The proposed method concentrates on more on security and to achieve less network complexity. This is done by using a CBSDV scheme in which all the data of the nodes entering into a network or exiting from the network are maintained by Credibility Check Table (CCT) and update automatically. Here, secure data transmissions in MANETs are obtained with the help of an efficient routing protocol and cryptographic keying technique. Two steps are involved, first routing and then cryptographic keying for protection of packets in the transmission.

Further the Packet Delivery Ratio increases, the delay decrease, thereby decreasing the network complexity.

The rest of the paper is organized as follows. The current chapter gives the literature survey and problem definition. Section 2 gives a brief description of the proposed system model. Section, 3 gives a research methodology. Performance analysis is illustrated in Sect. 4, result in Sect. 5. Finally concluding remarks are given in Sect. 6.

2 System model

The system model of the Fig. 1 shows the proposed methodology as well as it is divided into three steps.

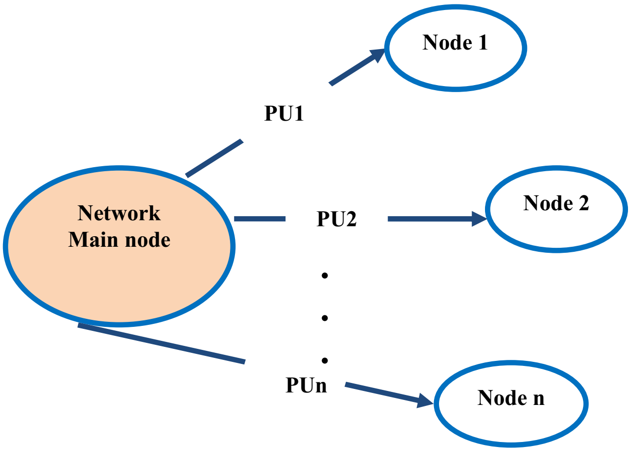
Step 1 In this, the main node creates a public key and sends to all the nodes present in the network to initialize the process. The system model of the network consists of 27 nodes. Assuming that 27th node generates the common public key to all other nodes, and it initializes.

In step 2, node 0 broadcasts the route request to neighbor nodes. Here the nearest neighbor node is node 1. Node1 once receive the request, send the acknowledgement to node 0. Then the node 0 will be initialized for its more process.

In step 3, by using CBSDV technique node 0 checks node 1's qualifications by matching it with the "Credibility Check Table". If it does match with that table, then node 1 is said to be malicious and it drops that node. If it matches, it performs the curve function which is $y = ax^2 + bx + c$ and then substitute the values in $S = (x^2 - x^1)/(y^2 - y^1)$.

Let this value be S. If S is greater than the threshold value for single node, node 1 is said to be malicious and it will be dropped out. If the value of S is less than or equal to the threshold value for single node the encrypted message along with the encrypted secret key of node 0 will be sent to node 1. Now node 1 will proceed the communication.

Step 1 Main node generates the public key



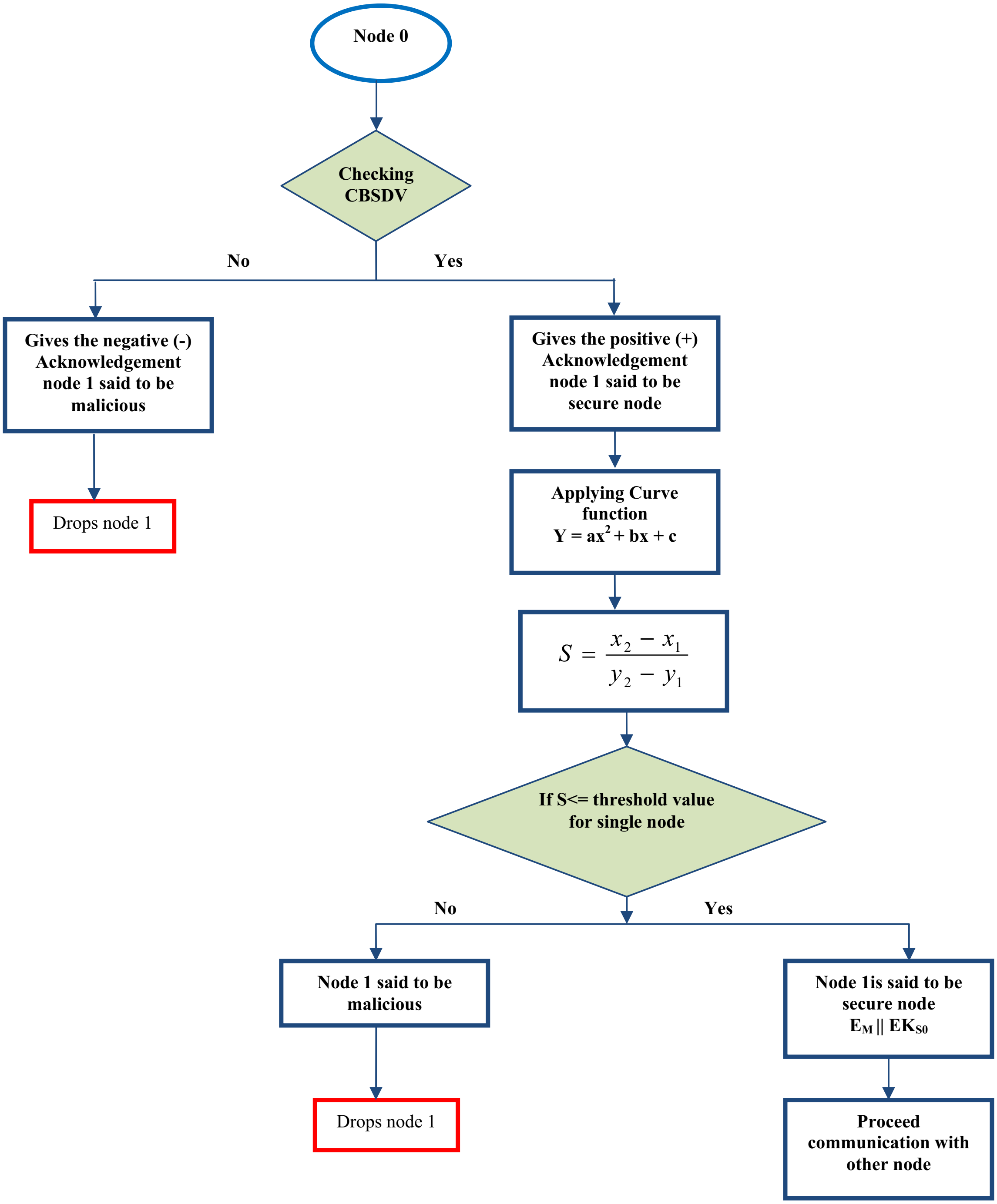
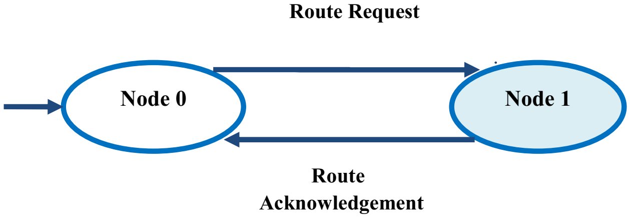

Node 0
Checking CBSDV
No
Yes
Gives the negative (-) Acknowledgement node 1 said to be malicious
Drops node 1
Gives the positive (+) Acknowledgement node 1 said to be secure node
Applying Curve function
$Y = ax^2 + bx + c$
$S = \frac{x_2 - x_1}{y_2 - y_1}$
If S<= threshold value for single node
No
Yes
Node 1 said to be malicious
Drops node 1
Node 1is said to be secure node
$E_M \| EK_{S0}$
Proceed communication with other node

Fig. 1 Proposed methodology (step 1, step 2, step 3)

Step 2 Node sends route request and gives acknowledgement



Step 3 Checking with credibility check table and applying curve based cryptography for security

3 Research methodology

In this proposed methodology, two techniques are considered such as CBSDV routing protocol and curve based cryptography that gives security in wireless MANET. The hashing function is used and its speciality is that every node changes its secret key after sharing its keys to the corresponding nodes in achieving maximum security, which is described in below.

3.1 Routing protocol

For node to node communication CBSDV routing protocol is used, which is a table based routing protocol. CCT is a subpart of CBSDV on which the source node collects all the information about the nearby one such as hop count, time taken, energy values and the trust scores (credibility score) of the communication networks. Three conditions have to be satisfied for achieving a good credibility score are as follows:

1. The node should be already an existing node.
2. The node should be the shortest route while travelling from source to destination.
3. When the source sends the 'test' message to a particular node, it has to finish the transmission to its neighbour node within a specific time limit.

Table 1 shows an example of source node CCT as well as Fig. 2 depicts the working process of CBSDV and CCT, Fig. 3 shows the algorithm for CBSDV. It can be clearly seen that for node A1 routing concept, the number of hops is 3, credibility score is the maximum which is 46 and the sequence time is 001000 ms. For node A4 and node A6 routing concepts, the number of hops are 2 and 1, credibility scores are 36 and 26, for the sequence time 001200 and 001500 respectively.

Figure3 shows about the algorithm for CBSDV. It shows about how the hash function secures the data while at transferring. The Credibility Vector Table (CVT) updates and checks the information of each transmission once the node enters into the network. If it matches allow transferring the data for transmission else it drops the data.

Here for understanding three paths are taken for transfer of data from source to the sink node. Figure 4 shows the routing concept using three paths. The first path is source, A1,A2, A3, sink. The second path is source, A4, A5, sink. The last path is source, A6, sink.

3.2 Cryptographic technique used for data security

To secure data from external attacks, we need a security algorithm to protect the data from being decrypted by an attacker node. The security algorithm used for this purpose is curve based cryptographic technique.

3.3 Curve based cryptography keyin

It is a public key cryptographic technique which can be also said as two-key cryptography technique. The encryption is done by curve function and the curve, which is used for encryption is sent only to genuine nodes. In this method the key value's i.e. both public and private key will be encrypted on another curve function equation. For example curve equation of a parabola is written as

$$y = ax^2 + bx + c \tag{1}$$

where a, b are the co-efficient of the parabola and C is a constant value which are the values sent as the public key. A, B are intercepts of the parabola.

Consider, for example: a = 2, b = 4. And c = 5 in this case.

For calculating the value of the slope (Which is the secret key), a line has to be drawn connecting the origin (−1, 3) and (0, c) the value of c is 5 in this equation.

The slope function of that curve will be given as.

$$S = \frac{x_2 - x_1}{y_2 - y_1}$$
$$S = \frac{0 - (-1)}{5 - 3}, \tag{2}$$

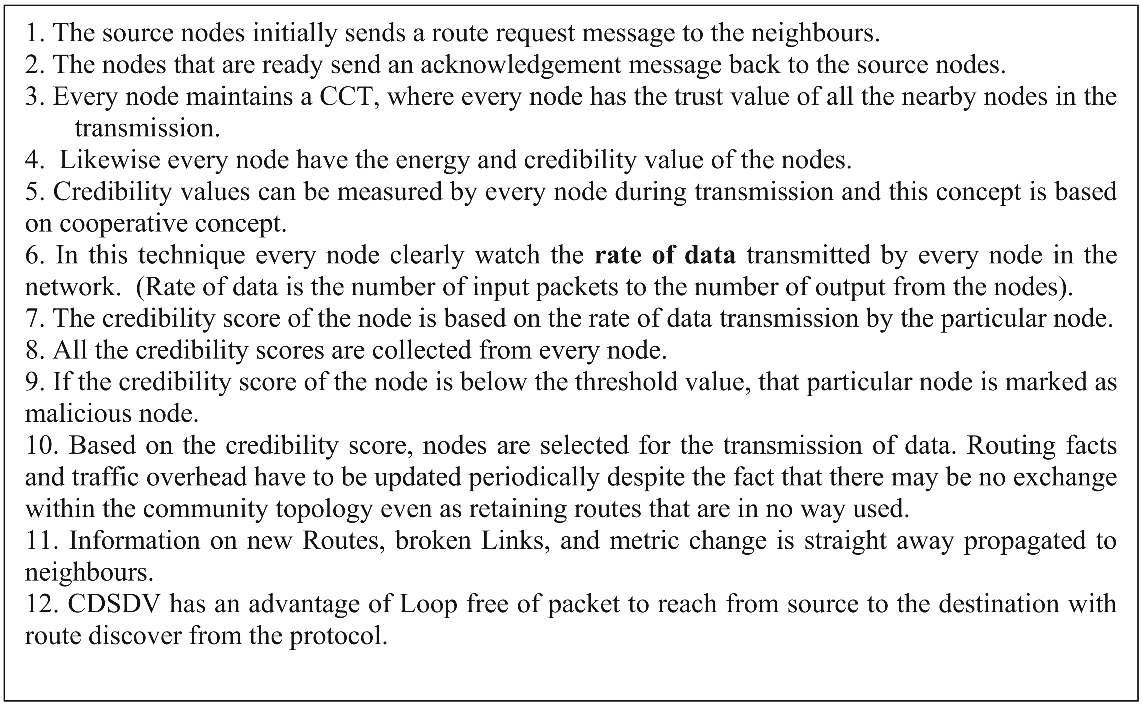
therefore the value of S is 0.5.

This is used as the secret key.

Figure 5 shows technique for the curve function used is a parabola, and the curve function which is used to encrypt the data has to be updated regularly. This increases the security of the encryption. By this way the curve function is updated regularly in a successful transmission made by the data. In this curve based cryptographic technique. Where x and y are the private keys and intercepts of the curve. a, b are the co-efficient values which act as the

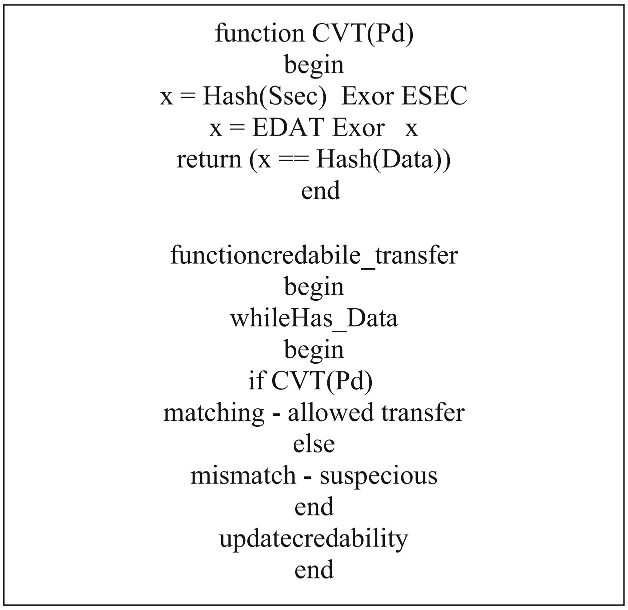
Table 1 Example of source node credibility check table (CCT)

Destination	Next hop	Number of hops	Credibility	Sequence time (ms)
Sink	A1	4	46	1000
Sink	A4	2	36	1200
Sink	A6	1	26	1500



1. The source nodes initially sends a route request message to the neighbours.
2. The nodes that are ready send an acknowledgement message back to the source nodes.
3. Every node maintains a CCT, where every node has the trust value of all the nearby nodes in the transmission.
4. Likewise every node have the energy and credibility value of the nodes.
5. Credibility values can be measured by every node during transmission and this concept is based on cooperative concept.
6. In this technique every node clearly watch the **rate of data** transmitted by every node in the network. (Rate of data is the number of input packets to the number of output from the nodes).
7. The credibility score of the node is based on the rate of data transmission by the particular node.
8. All the credibility scores are collected from every node.
9. If the credibility score of the node is below the threshold value, that particular node is marked as malicious node.
10. Based on the credibility score, nodes are selected for the transmission of data. Routing facts and traffic overhead have to be updated periodically despite the fact that there may be no exchange within the community topology even as retaining routes that are in no way used.
11. Information on new Routes, broken Links, and metric change is straight away propagated to neighbours.
12. CDSDV has an advantage of Loop free of packet to reach from source to the destination with route discover from the protocol.

Fig. 2 Working process of CBSDV and CCT



```
function CVT(Pd)
begin
x = Hash(Ssec)  Exor ESEC
x = EDAT Exor   x
return (x == Hash(Data))
end

functioncredabile_transfer
begin
whileHas_Data
begin
if CVT(Pd)
matching - allowed transfer
else
mismatch - suspecious
end
updatecredability
end
```

Fig. 3 Algorithm for CBSDV

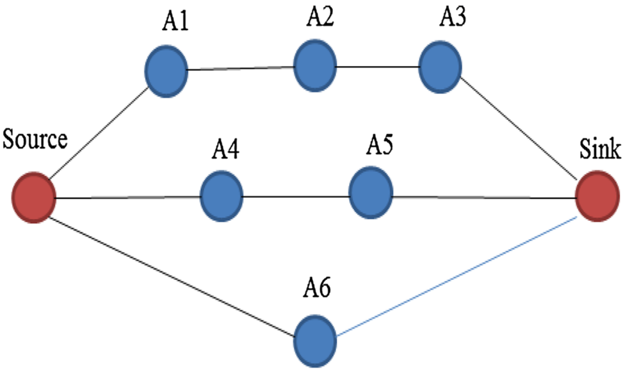


Fig. 4 Routing concept using three paths

public key. ‘K’ is the number of bits that are transferred from the sender. The sender sends the message with a public key to all the nodes surrounding the sender node and the receiver node decrypts the message.

Figure 6 illustrates the steps for curve based cryptography. Every node assigns a hash function (Curve function) that can be encrypted with true nodes in the transmission. The nodes that cannot decrypt the message is assigned as malicious nodes. To detect whether the node has taken part in the transmission, the key hashing methods has to be updated regularly. This removes the effect of malicious nodes entering into the transmission.

4 Performance analyses

The proposed KEY mode technique performance is analyzed by using three types of modes called ACK, SACK and MRA. The number of wireless nodes for ACK, SACK and MRA are 25 whereas in key mode it is 27. The network size is assumed to be same for all the modes. For the existing modes which are ACK, SACK and MRA the protocol used is AODV whereas it is CBSDV for key mode. Table 2 shows that the range of node communication for ACK, SACK, MRA and KEY modes are 500, 900, 1000 and 1000 m respectively. Maximum transmission of data is achieved only in KEY mode which is 100 to 900 m. Similarly, maximum throughput and bandwidth are achieved in the KEY mode which are 100 mbps and 1000 mbps respectively. The frequency and packet transmission are maintained the same for all the modes which are 50 Hz and 1000 bytes respectively. KEY mode has the highest packet rate which is 1000 mbps. As far as the request message interval is concerned, it is 10–20 s for the KEY mode which is an added advantage. Finally, the simulation time is achieved to be the same for all the modes which is 2000 s.

5 Results

The data transmission of the proposed methodology which is CBSDV along with the EC is compared with existing methodology which are EAACK (RSA) and EAACK (DSA). The results are discussed as follows.

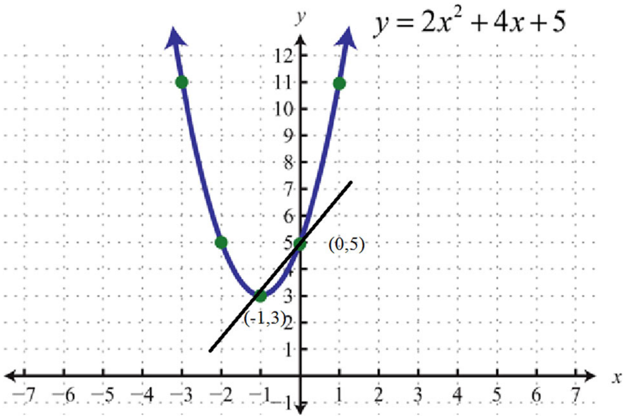
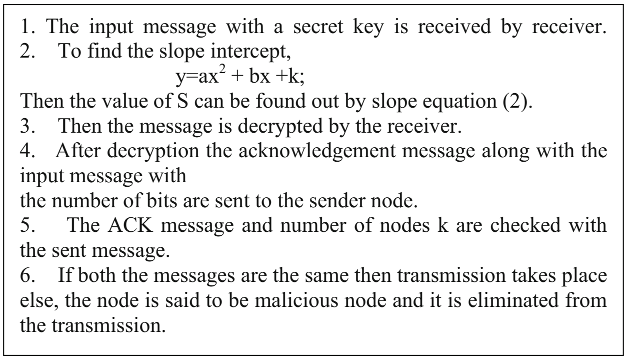


Fig. 5 Example of curve based cryptography



1. The input message with a secret key is received by receiver.
2. To find the slope intercept,

$$y=ax^2 + bx +k;$$

Then the value of S can be found out by slope equation (2).
3. Then the message is decrypted by the receiver.
4. After decryption the acknowledgement message along with the input message with
the number of bits are sent to the sender node.
5. The ACK message and number of nodes k are checked with the sent message.
6. If both the messages are the same then transmission takes place else, the node is said to be malicious node and it is eliminated from the transmission.

Fig. 6 Steps for curve based cryptography

Figure 7 Shows the time versus delay of transmission graph. X-axis denotes the number of users performing the communication and Y-axis is the time taken for delay of transmission. First of all end–end delay transmission is calculated and the data is transmitted without applying the key. The transmission with the key and the throughput for 20 users are 13 and 12.5 ms respectively, both decrease as the number of users increase. For 150 and 200 users they increase and reach 11.5 and 10.5 ms respectively. i.e. for 150 users the delay is very less which is a positive one. As far as end–end-delay is concerned, it also decreases initially, but there is a sudden increase when the number of users are 200. This shows that there is a malicious activity or packet drops at the point 13 ms. Finally the number of users increase and there is a gradual decrease in latency which is 11 ms. Therefore, the malicious node is found in this process.

Figure 8 shows time versus PDR. The Packet Delivery Ratio is the ratio of number of packets received to the number of packets sent. The graph shows the latency of communication. From the above graph it can be clearly seen that the data transmission with the key and the throughput for 20 users are 13 and 12.5 ms respectively, both decrease as the number of users increase. For 150 and 200 users they increase and reach 11.5 and 10.5 ms respectively. i.e., for 150 users the delay is very less which is a positive one. As far as end to end delay is concerned it also decreases initially, but there is a sudden increase when the number of users are 200. This shows that there is a malicious activity or packet drop at the point 13 ms.

Finally the number of users increase and there is a gradual decrease in latency which is 11 ms. As a result malicious is found in this process.

$$PDR = \frac{No\ of\ packets\ received}{No\ of\ packets\ sent} \quad (3)$$

Equation (3) says that generally packet delivery ratio is nothing but the number of packets received is divided by number of packets sent. The packet delivery ratio increases

Table 2 Proposed technique CBSDV with key mode

S. no	Parameters	Type of mode			
		ACK	SACK	MRA	KEY
1	Number of wireless nodes	25	25	25	27
2	Network size	1700 × 800	1700 × 800	1700 × 800	1700 × 800
3	Protocol usage	AODV	AODV	AODV	CBSDV
4	Range of node communication (m)	500 (100–200)	900 (300–600)	1000 (300–600)	1000 (100–900)
5	Throughput (mbps)	50	80	90	100
6	Bandwidth (mbps)	400	700	900	1000
7	Frequency range (Hz)	50	50	50	50
8	Packet transmission (bytes)	1000	1000	1000	1000
9	Packet rate (pps)	250	600	800	1000
10	Request message interval (s)	10–20	10–50	10–30	10–20
11	Simulation time (s)	2000	2000	2000	2000

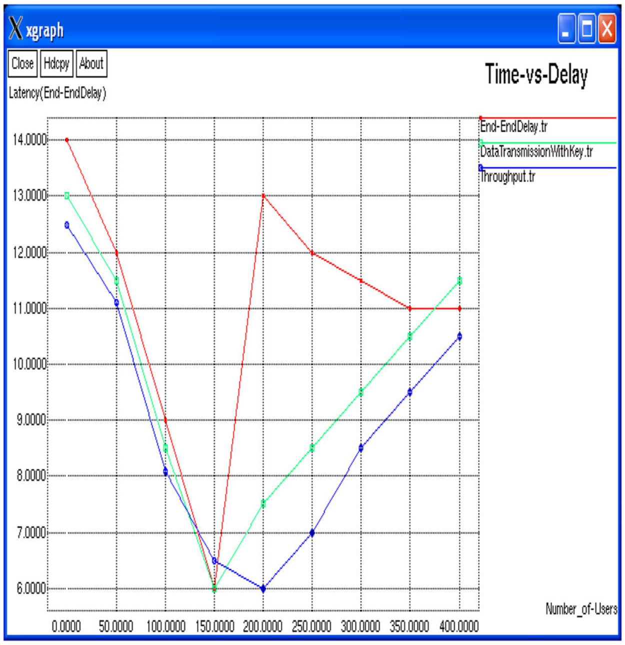


Fig. 7 Time versus delay of transmission graph

parallel with the increasing in secure key maintenance and verification of packet size level (i.e.) buffer size level. X-axis denotes the time (s) whereas Y-axis denotes the Packet delivery ratio. From the above graph it can be seen that as the time increases the data transmission with 'Time To Live' (TTL) keeps on decreasing until 150 s. But after 150 s it tends to increase faster and finally maintains a constancy of Packet delivery Ratio (PDR) of 13.5. The delay keeps on decreasing and maintains constancy at 2.5.

By using the unique secret key the data transmission takes place securely till the destination is reached even though there is a drop in the packets. By using the secret key mechanism, the packet delivery ratio is increased and also there is a reduction in the delay of transmission in the network.

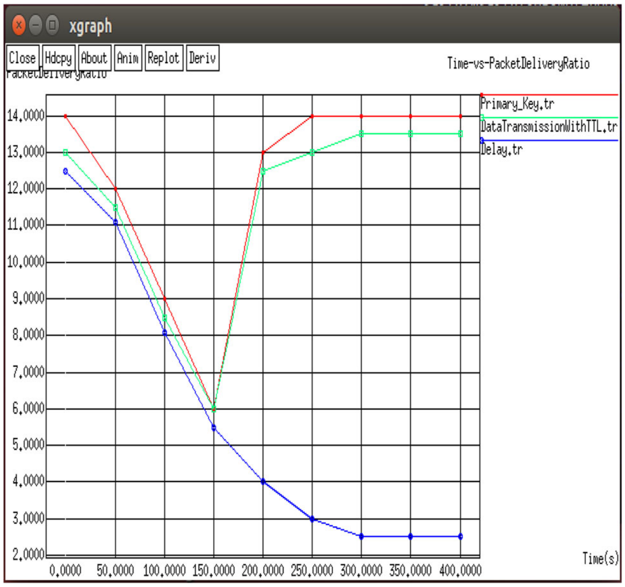


Fig. 8 Time versus packet delivery ratio (PDR)

Figure 9 shows the time versus throughput. X-axis denotes the number of user request and Y-axis denotes the throughput (Mbps) for increasing the Packet delivery ratio. The graph depicts that as a number of request increases, the data transmission with TTL and key maintenance increases and reaches a throughput of 9 and 6.9 respectively. Meanwhile as the number of request increases the buffer level verification also increases till a throughput of 6.2 is reached. But it maintains almost constancy and reaches a throughput of 6.9.

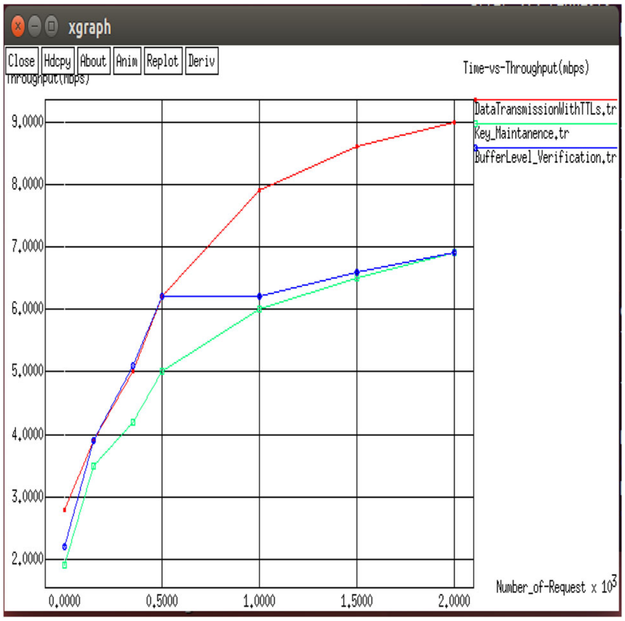


Fig. 9 Time versus throughput in communication

When the packet size increases or decreases from the initial packet size level, packet drop occurs in the secured network but the throughput detects the secure key and improves the throughput performance in the network.

6 Conclusion

In this paper, we have proposed an approach using CBSDV with Curve based cryptography along with Hashing function to improve the security level. whenever misbehavior occurs a unique key is generated, to achieve a secure transmission. since it is time-based key, it changes from time to time and it is easy to verify. To improve further, the key mode is used when the delay occurrence is found while dissatisfying the TTL and it also identifies the duplicate key in the network. CCT checks the data of every node and finds the malicious activity. The hashing function is used and it helps to update the secret key after the detection of every malicious activity. The encryption is done using the curve function in curve based cryptography, there is a chance of detecting the malicious activity. Therefore this proposed Cryptography techniques are used to hide the data Source Node ID, Packet Size, Node Location, and Destination Location and so on. Simulation results show that proposed scheme provides better secure network and CBSDV, hop count, time duration, energy values and trust scores decided the network performance between the source and destination in the network. However, this research work can be extended with energy harvesting and increasing the network lifetime.

References

1. Alinci, M., Inaba, T., Elmazi, D.: A fuzzy-based system for improving node security in MANET clusters. Int. Conf. Complex Intell. Softw. Intensive Syst. **1**, 390–401 (2016)
2. Alinci, M., Inaba, T., Elmazi, D.: Improving node security in MANET clusters: a comparison study of two fuzzy-based systems. Int. Conf. Complex Intell. Softw. Intensive Syst. **16**, 110–112 (2016)
3. Thorat, S.A., Kulkarni, P.J.: Uncertainty analysis framework for trust based routing in MANET. Int. J. Peer-to-Peer Netw. Appl. **2**, 220–233 (2017)
4. Krishna, S.R.M., Seeta Ramanath, M.N.: Security in MANET routing tables with FMNK cryptography model. IEEE Trans. Syst. Man Cybern. **12**, 121–132 (2015)
5. Manoj, V., Aaqib, M., Raghavendiran, N.: A novel security framework using trust and fuzzy logic in Manet. Int. J. Distrib. Parallel Syst. (IJDPS) **3**, 285–299 (2012)
6. Tarannum, R., Lamble, M.: Hybrid approach: detection of intrusion in Manet. Innov. Conf. Embed. Syst. Mob. Commun. Comput. **13**, 24–28 (2011)
7. Li, F., Yang, Y., Jie, W.: Attack and flee: game-theory-based analysis on interactions among nodes in MANETs. IEEE Trans. Syst. Man Cybern. **40**, 612–622 (2010)
8. Nagar, A., Jain, A.K.: On the security of non-invertible fingerprint template transforms. Int. Conf. Complex Intell. Softw. Intensive Syst. **50**, 99–104 (2009)
9. Yih-Chun, H., Johnson, D.B., Perrig, A.: 'SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. IEEE Workshop Mob. Comput. Syst. Appl. **55**, 415–426 (2002)
10. Anguswamy, R., Thiagarajan, M., Dagli, C.H.: Systems methodology and framework for problem definition in m obile ad hoc networks. IEEE Int. Syst. Conf. **33**, 312–324 (2008)
11. Ang, R., Safavi-Naini, R.: Cancelable Key-based Fingerprint Templates. University of Wollongong, Wollongong (2005)

N. Sridevi is a Research Scholar at the Department of Electronics and Communication Engineering in Adhiparasakthi Engineering College, India. She received her B.E., and M.E. in Computer Science and Engineering from Anna University, India. Her research interests include Mobile Ad hoc Networks, with Network Security.

V. Nagarajan is a Professor, Department of Electronics and Communication Engineering in Adhiparasakthi Engineering College, India. He received his B.E., from Madras University, India. He received his M.Tech. and Ph.D. from Pondicherry Engineering College, India. He is a member in IEEE, ISTE, IETE, IASTE and IAE. He has published more than 150 papers in national and international conferences/journals. His research interests include wireless communication, mobile communication and signal processing.