ISSN:0975-9646

Eigen Reputation One Hop Certificate Exchange for Secure and Self Organizing Key Management in Manet

Chidambar P.Inamdar
Research Scholar,
Bharathiar Uninversity, Coimabatore

Dr. C .Chandrasekar
Professor,
Periyar University, Salem

Abstract-Mobile node communication lies at the core for applications such as disaster relief operations, intelligent transportation system that aim at enhancing the safety and efficiency of transportation systems. As it does not rely on any fixed infrastructure and all networking functions has to be performed in a self-organizing manner, securing mobile ad hoc networks become a challenging issue, due to the absence of centralized services, key exchange and so on. This paper introduces a framework called Secure and Self Organizing Key Management (S-SOKM). The framework takes advantage of the self organized structure that does not require trustworthy network and therefore ensures secure way of communication between the nodes in network. To offer higher amount of security at low average end to end delay, an Eigen Reputation model is proposed. The Eigen Reputation model evaluates the trust based on the neighbour node's reputation and forwards the data packets according to the reputation count. In addition, one hop certificate exchange is performed to reduce the computational complexity and therefore increase the delivery ratio. Thus S-SOKM offers secure form of network. Experimental results exhibit consistency with the theoretical analysis, and show that S-SOKM achieves better security and lowers average end to end delay to other self organizing key structure. Also, S-SOKM achieves comparable data delivery efficiency to the state-of-the-art works.

Keywords: Mobile Ad hoc networks, Self Organizing, Key Management, Certificate exchange, Eigen Reputation

1. INTRODUCTION

Mobile ad hoc network with their self organizing property and high topology changes imposes security constraints to the mobile nodes in the network during data transmission. Many researchers have contributed towards security in MANET. A cooperative key agreement model [1] was designed to improve the security based on the secure secret key agreement protocol. However, in addition to the benefits it brings to mobile ad hoc network, communication and processing overhead also raises some practical issues. To address these issues, secure payment scheme with communication and processing overhead [2] was designed with the aid of evidence aggregation technique. However, the assumption that the nodes provide valid evidences cannot be held for efficient data acquisition. A method to provide secure and efficient data dissemination framework was introduced in [3]. Securitizing the network through anonymity was introduced in [4].

The concept of encryption using attributes is considered to be a promising approach that satisfies the requirements for secure data retrieval. In [5], Cipher Text Policy Attribute Based Encryption was investigated for secure data retrieval. However, the problem of applying the attributed based encryption imposed several problems that mainly depended on the other nodes in the network. A solution to this was provided in [6] by introducing multiple one-way key chains that not only improved security but also reduced the communication overhead to obtain the key. Another method introduced in [7] provided an insight into temporal and spatial correlated channel coefficient that ensured key agreement.

Considering the unique features of mobile ad hoc networks, the key management mechanisms to ensure security in the conventional network models are not specifically suitable to mobile ad hoc networks. Therefore, methods designed specifically for mobile ad hoc networks aiming at improving the security and data delivery ratio, are necessary.

This paper considers the use of secure and self organizing key management framework for data packet transmission based on the public key certificate validity and Eigen reputation model. The work begins by using a simple public key certificate validity model to examine the neighboring nodes and to verify the existence of an efficient validity approach able to generate public key certificate. The work introduced an eigen reputation model for measuring the reputation and trust of the corresponding neighboring nodes and data packet transmission using one hop certificate exchange model.

The remainder of this paper is organized as follows. Section 2 reviews the related works. Section 3 presents S-SOKM framework. Security analysis and performance evaluation is given in Sections 4. Section 5 provides the concluding remarks.

2. RELATED WORKS

Security in mobile ad hoc networks can be provided either using a single authority domain or through full self-organization. In [8], security for vehicular networks was introduced within a game theoretic framework using input centrality measures based on single authority domain. In [9], a random network model with the neighboring nodes possessing primary security association was introduced to improve the throughput based on self organized public key scheme. A secure high throughput multicast mechanism for wireless mesh network was introduced in [10] using a measurement and accusation based technique.

Reliable data delivery using key management in MANET has received great attention due to the self organized nature of the network. In [11], a reliable data delivery model using Virtual Destination-based Void Handling was introduced ensuring security. Another method introduced in [12], discovered and verified the neighbor positions before sending data, reducing the attack

rate. A key generation process used in [13] provided an insight into secure communication for exchanging information using fuzzy-cryptography scheme. A probabilistic key distribution model used in [14] also ensured security using Hash Message Authentication Code (HMAC).

Whenever symmetric cryptography technique is used in ad hoc network, public keys of the nodes need to be made available in a secure manner. In [15], public key on regular nodes were cached to provide fault tolerant mechanisms and also ensured mechanisms to protect against attacks. A secure collaborative key management was introduced in [16] to ensure security using Diffie Hellman assumption.

In [17], a secret sharing key mechanism was investigated to reduce the energy consumption reducing the high possibility of common keys. Secure data communication through cipher based scheme [18] was introduced to ensure real time data transmission using chaotic stream cipher-based cryptography scheme. Group key agreement scheme [19][20] used public key certificate management for not only improving the security but also reduced the consumption of resources during certificate verification process.

Comparing with previous works, our solution adopts a secure and self organizing key management framework and improves the security and therefore the data delivery ratio. Also, we ingeniously use the public key certificate validity to validate the certificate of the corresponding neighboring nodes, which reduces the average end to end delay.

3. SECURE AND SELF ORGANIZING KEY MANAGEMENT

3.1 Problem statement

Let us consider a graph '$G = (V, E)$' where 'V' represents the vertices and 'E' represents the edges of with the graph 'G' called as the key exchange graph. The vertices of the key exchange graph represent public keys whereas the edges represent one hop certificates. A one hop certificate chain from a public key 'Key_a' to another public key 'Key_b' is denoted by a directed path from vertex 'Key_a' to vertex 'Key_b' in key exchange graph 'G'. Now the problem is stated as follows. With the key exchange graph, a secure and self organizing key management framework for improved data delivery ratio with reduced average end to end delay is designed. Figure 1 shows the block diagram of secure and self organizing key management framework.

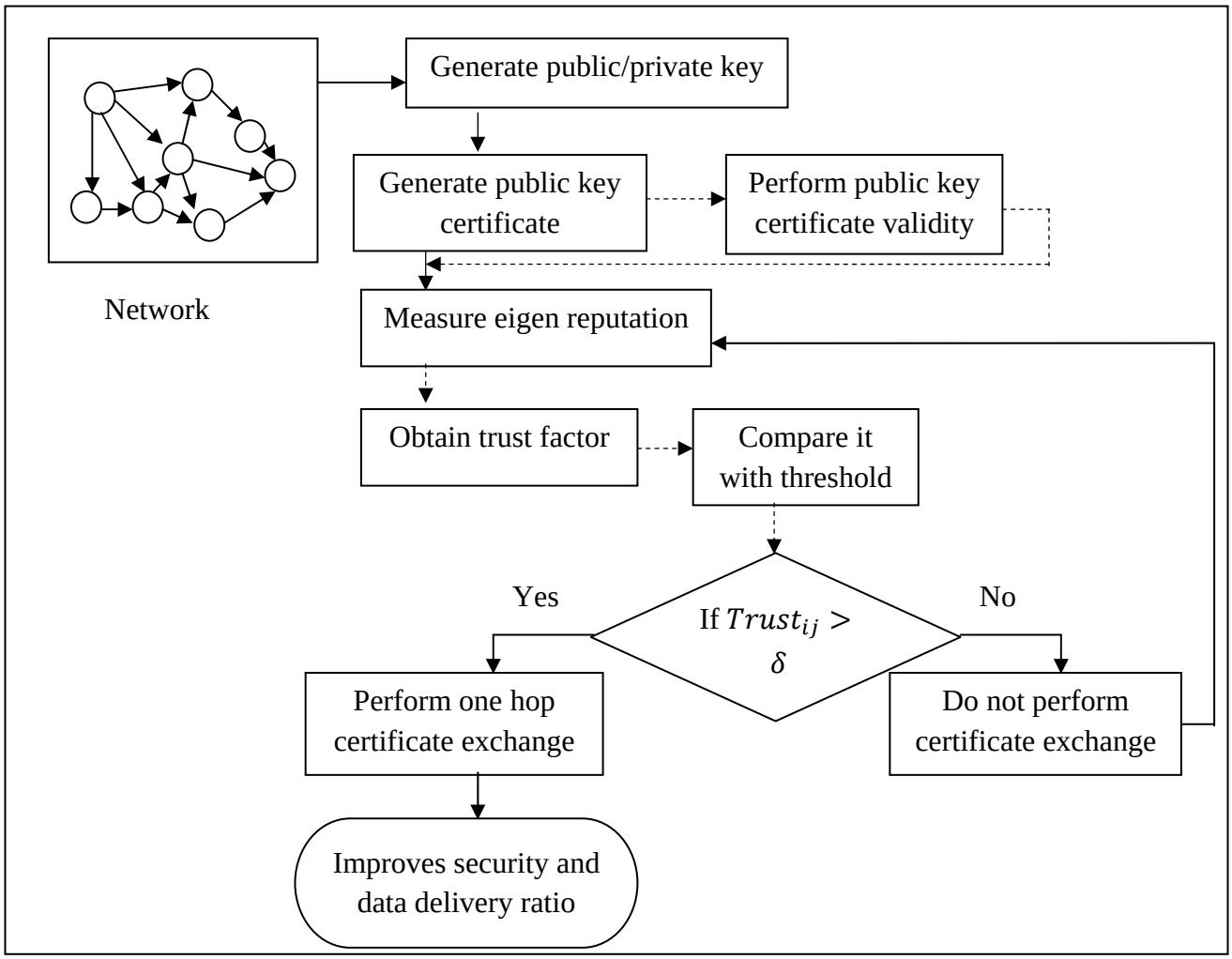

Figure 1 Block diagram of secure and self organizing key management framework

As illustrated in figure 1, the considered S-SOKM improves security and data delivery ratio through three phase model, namely, key generation, Eigen Reputation Trust Management model and One Hop Certificate Exchange. The Key Generation model includes the generation of public/private key of the mobile nodes in a self organizing manner. The Eigen Reputation Trust Management model obtains the reputation and trust of each mobile node and accordingly to the trust factor, one hop certificate exchange is performed.

3.2 Key generation

The first step towards the design of Secure and Self Organizing Key Management framework is the generation of public/private key. The public key and the equivalent private key of each mobile node in MANET are created by the corresponding mobile node itself. Let us consider two mobile nodes 'MN_i' and 'MN_j'. If the mobile node 'MN_i' believes that a public key 'Key_j' belongs to another mobile node 'MN_j', then the mobile node 'MN_i' grants a public key certificate in which 'Key_j' is bound to 'MN_j' by the signature of 'MN_i'. It is mathematically formulated as given below.

$$MN_i \rightarrow MN_j : \ Key_j \ \forall \ MN_j, (i \ \in 1,2, \dots, n) \quad (1)$$

The public key certificates 'Key_c' consist of the public key, public key issuing time '$Issue_t$' and public key expiring time and '$Expiry_t$' respectively.

$$Key_c \rightarrow \ Key_i, Issue_t, Expiry_t \quad (2)$$

The public key issuing and expiry time in (2) is used in S-SOKM framework to avoid the mobile node pair being held by the network for longer duration of time. When a public key certificate expires (meets the '$Expiry_t$') and the issuing mobile node believes that the certificate is still valid, the issuing mobile node issues an updated version of the same certificate. The updated version includes old public key certificate but with the updated public key issuing and expiring time '$UIssue_t$' and '$UExpiry_t$' respectively. The updated version is mathematically formulated as given below.

$$UKey_c \rightarrow Key_i, UIssue_t, UExpiry_t \quad (3)$$

From (3), the updated public key certificate is evaluated that in turn reduces the average end-to-end delay of key generation. Figure 2 shows the Key Generation algorithm.

The key generation algorithm as shown above involves the generation of public/private key pairs using self organizing key framework. This framework allows the mobile nodes to generate their own public/private key pairs. The performing mobile nodes (that has to send data packets) issue public key certificates based on the other mobile node's public keys.

To avoid the mobile nodes to exploit the network entirety, issuing time and expiry time is provided by the mobile node. Whenever the expiry time is reached, the process is continued but with the updated issue and expiry time. In this way, average end-to-end delay between the mobile nodes for key generation is minimized.

Input: Mobile Nodes '$MN_i = MN_1, MN_2, \dots, MN_n$', Public Key '$Key_i = Key_1, Key_2, \dots, Key_n$', public key issuing time '$Issue_t$', public key expiring time '$Expiry_t$'
Output: Optimizes end-to-end delay
Step 1: Begin Step 2: For each Mobile Nodes 'MN_i' Step 3: Evaluate public key certificate using (2) Step 4: If (public key expiring time = '$Expiry_t$') Step 5: If (public key certificate valid) Step 6: Evaluate updated version of public key certificate using () Step 7: Else Step 8: Public key invalid Step 9: End if Step 10: Else Step 11: Go to step 3 Step 12: End if Step 12: End for Step 13: End

Figure 2 Key Generation algorithm

3.3 Eigen Reputation Trust management

The second step towards the design of Secure and Self Organizing Key Management framework is the Eigen Reputation Trust management model. The Eigen Reputation Trust management in S-SOKM framework is applied with the objective of validating the mobile nodes in the network.

The trust management is evaluated with the aid of Eigen Reputation factor. Each mobile node in the network measures the Eigen Reputation factor of its neighbourhood mobile nodes. This is performed with the objective of measuring the reputation of the nodes and therefore improving the security. Let 'MN_i' be the neighboring node of 'MN_j'. Then the Eigen Reputation Factor 'ERF_i' of its neighboring nodes is mathematically evolved as given below.

$$ERF_i = \sum_{i=1}^{n} NN_i ERP_j \quad (4)$$

Where 'NN_i' is the neighboring nodes of the network with 'n' symbolizing the total number of mobile nodes in the network. Once the neighboring nodes reputation is evaluated using the Eigen Reputation Factor, the trust value for the corresponding node is obtained. In

order to evaluate the trust value '$Trust_{i,j}$', the difference between the percentages of data packets forwarded '$DPF_{i,j}$' to the percentage of data packets dropped '$DPD_{i,j}$' over the total number of data packets ' DP_n ' offered to the neighboring nodes 'NN_i' is measured. Here '$DPF_{i,j}$' is the percentage of data packets initiated 'DPI' from 'MN_i' that was forwarded 'DPF' by 'MN_j' over the total number of data packets provided to 'MN_j'.

$$\sum_{i,j=1}^{n} DPF_{i,j} \rightarrow \frac{DPF(MN_j)}{DP_i} \qquad (5)$$

On contrary, '$DPD_{i,j}$' is the percentage of data packets that were dropped 'DPD' over the total number of data packets provided to 'MN_j'.

$$\sum_{i,j=1}^{n} DPD_{i,j} \rightarrow \frac{DPD(MN_j)}{DP_i} \qquad (6)$$

Finally, trust management is performed with each of its direct neighbor nodes with the aid of the above '$DPF_{i,j}$' and '$DPD_{i,j}$' respectively.

$$Trust_{i,j} = DPF_{i,j} - DPD_{i,j} \qquad (7)$$

From (7), the Eigen Reputation Trust management is evolved for any mobile nodes. With the obtained trust value of the neighboring nodes, the decision regarding the data packet forwarding is made in an efficient manner, thereby improving the security factor. Figure 3 shows the Eigen Reputation Trust algorithm aiming at improving the security during data forwarding.

As shown in the algorithm, with the objective of improving the security, for each mobile node, the reputation of the neighboring mobile node is measured. The reputation of the neighboring node is obtained through data packet forwarding and data packet drop rate. Followed by this, the measure of trustworthiness is obtained by assigning a threshold factor. Comparison with this threshold factor to the resultant output obtained from reputation measures the trustworthiness of mobile node. With this, the neighboring nodes through which data packets are forwarded through one hop certificate exchange are obtained. This in turn improves the security during data forwarding.

Input: Mobile Nodes '$MN_i = MN_1, MN_2, \dots, MN_n$', Public Key '$Key_i = Key_1, Key_2, \dots, Key_n$', Threshold '$\delta$'
Output: Improved security

```
Step 1: Begin
Step 2:      For each Mobile Nodes 'MN_i'
Step 3:           If (MN_i is neighbour to the MN_j th node)
Step 4:             NN_i = 1
Step 5:                  Measure Data Packet Forwarding Rate using (5)
Step 6:                  Measure  Data Packet Drop Rate using (6)
Step 7:                  Measure trust factor using (7)
Step 8:                  If Trust_{i,j} > δ
Step 9:                       Neighboring nodes are highly secured nodes
Step 10:                        Perform certificate exchange through neighboring nodes
Step 11:                 Else
Step 12:                      Neighboring nodes are not secured nodes
Step 13:                      Do not perform certificate exchange
Step 14:                 End if
Step 15:           Else
Step 16:                NN_i = 0
Step 17:                Go to step 3
Step 18:           End if
Step 17:      End for
Step 18: End
```

Figure 3 Eigen Reputation Trust algorithm

Input: Source node ' SN ', Mobile Nodes ' $MN_i = MN_1, MN_2, \dots, MN_n$ ', Public Key '$Key_i = Key_1, Key_2, \dots, Key_n$', Destination node '$DN$', Data Packets '$DP_i = DP_1, DP_2, \dots, DP_n$'
Output: Optimizes data delivery ratio

```
Step 1: Begin
Step 2:      For each Mobile Nodes 'MN_i'
Step 3:           If 'MN_i' has not certificates of 'DN'
Step 4:                Then 'MN_i' forwards 'DP_i' to neighbour nodes
Step 5:           Else 'MN_i' forwards 'DP_i' to 'SN' to obtain public key certificate
Step 6:           End if
Step 7:      End for
Step 8: End
```

Figure 4 one hop certificate exchange algorithm

3.4 One Hop Certificate Exchange (ref 4) (Improves delivery ratio)

Finally, the one hop certificate exchange in Secure and Self Organizing Key Management framework helps the mobile nodes to authenticate themselves with the neighboring mobile nodes in the network before they perform data packet transmission.

In order to improve the reliability of Eigen Reputation Trust Management, One Hop Certificate Exchange mechanism is adapted in S-SOKM framework. During the One Hop Certificate Exchange, the public key of a node is certified by the one hop mobile nodes through certificate exchange. As a result of One Hop Certificate Exchange, the confidence assigned to the certificates is higher. Moreover, the authentication is performed mutually, improving the delivery ratio. Figure 4 shows the one hop certificate exchange algorithm

The one hop certificate exchange algorithm performs authentication with the aim of improving the delivery ratio through corresponding neighboring nodes. According to the public key certificate, if the mobile source node has certificates (public key certificate) of DN, the data packets are forwarded to the neighboring nodes. On contrary, with no certificates obtained from the neighboring nodes, the mobile nodes forward data packets to the source node to iterate once again with the objective of acquiring the certificate. In this way, the mobile nodes send their data packets only to the neighboring nodes possessing certificates. In this way not only security is improved but also the data delivery ratio.

4. EXPERIMENTAL SETTINGS

This section evaluates the proposed secured data delivery framework through simulation results by adopting NS2 simulator. Study presents the performance of the Secure and Self Organizing Key Management (S-SOKM) framework and compares with its traditional Cooperative Key Agreement (CKA) [1] and Secure Payment Scheme (SPS) [2] for Mobile Ad hoc network.

To evaluate the performance of S-SOKM framework, a network consisting of 70 mobile nodes within the 1500 * 1500 rectangular area using Random Waypoint Model as the mobile model is used. The source destination combination for S-SOKM framework is spread in the network in random form where the packet rate is set as 9, 18, 27,…, 63 packets / second. The mobile nodes in the network select a random speed between the minimum speed value 0m/s and a maximum speed of 35m/s. The simulation is conducted for S-SOKM framework with multiple instances of the mobile nodes and various routing modes in mobile ad hoc network. The metrics used in the evaluations are number of mobile nodes, average end to end delay, security and data delivery ratio for rendering self organizing key management framework.

4.1 Impact of average end to end delay

The average end to end delay is the product of time taken to obtain the public/private key to the number of mobile nodes in the network.

$$AEED = \sum_{i=1}^{n}(Time(Key_i) * MN_i) \qquad (8)$$

Where '$AEED$' symbolizes the average end to end delay and 'MN_i' represents the mobile nodes in network. The average end to end delay is measured in terms of milliseconds.

Table 1 Tabulation for average end to end delay

Mobile nodes	Average end to end delay (ms)		
	S-SOKM	CKA	SPS
10	0.35	0.48	0.55
20	0.52	0.65	0.72
30	0.68	0.81	0.88
40	0.48	0.61	0.68
50	0.61	0.74	0.81
60	0.78	0.81	0.88
70	0.65	0.78	0.85

The table 1 represents the average end to end delay obtained using NS2 simulator and comparison is made with two other methods, namely CKA [1] and SPS [2].

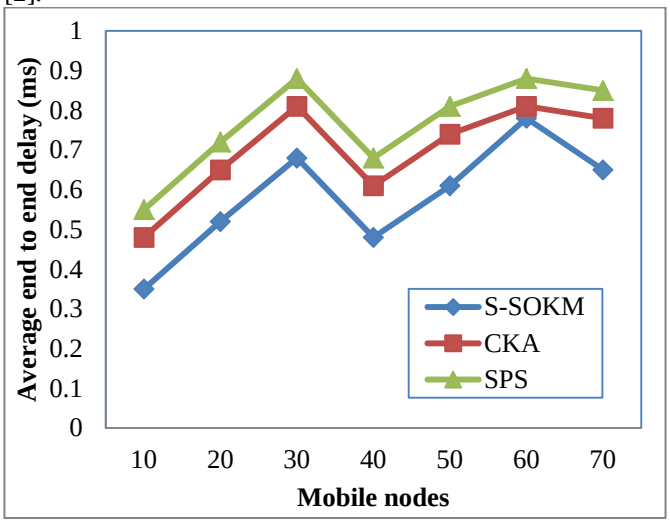

Figure 5 Measure of average end to end delay

Figure 5 illustrates the average end to end delay for key generation versus number of mobile nodes in the network. As shown in the figure, the average end to end delay rate is proportional to the number of mobile nodes. With the increase in the simulation time, number of mobile nodes to obtain the public key also increases, the S-SOKM framework reduces the average end to end delay compared to CKA [1] and SPS [2]. At the same time, the average end to end delay observed is not linear and varies due to the change in topology resulting in the mobile node positional changes.

From results, we observed that as the number of mobile nodes increases though average end to end delay increases, comparatively the performance of S-SOKM framework is better than that of CKA by 21.92% and SPS by 34.72%. Here the S-SOKM framework reduces the average end to end delay as we are performing Self Organized Key Management based on the Key Generation algorithm that obtains the public/private key through updated public key at reducing the number of transmissions. As a result, it reduces the average end to end delay for key generation and therefore transmit the total packets to the destination in an efficient manner.

4.2 Impact of security

Security with respect to data packets being forwarded is measured on the basis of data packets received by the neighboring node in MANET. Therefore, security is the difference between the total packets sent to the packets not received by the neighboring node.

$$S\,(DP) = DP_s - DP_{nr} \qquad (9)$$

From (9), 'DP_s' refers to the data packets sent and 'DP_{nr}' refers to the data packets not received by the neighboring node in MANET. It is measured in terms of packets per second (pps).

Table 2 Tabulation for security

Data Packets Sent	Security (pps)		
	S-SOKM	CKA	SPS
9	7	6	5
18	13	11	9
27	21	18	15
36	31	28	24
45	39	35	32
54	48	45	40
63	57	52	48

Table 2 represents the comparison results of security and performance with 70 mobile nodes with an average of 63 data packets sent for simulation purpose.

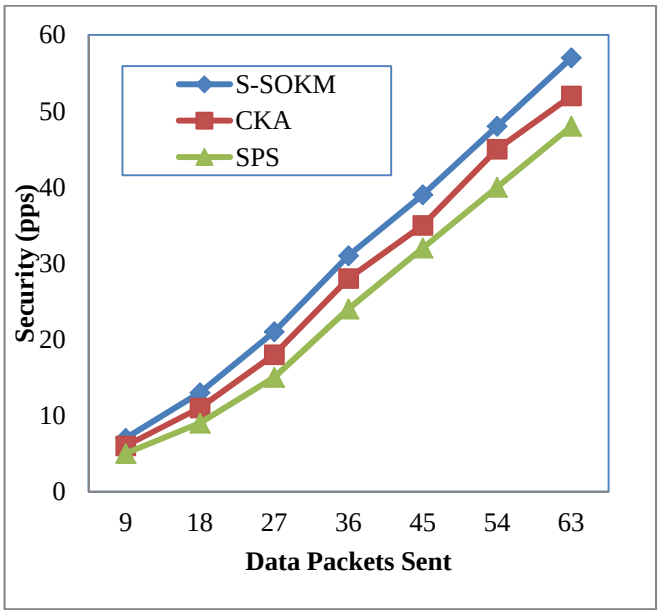

Figure 6 Measure of security

Figure 6 shows the quantitative results to compare the security performance of the three methods. To investigate the impact of security, we ran a simulation varying the number of mobile nodes and data packets being sent in the network. Specifically we fix the maximum speed of mobile node to 25 m/s and vary the number of mobile nodes from 10 to 70. Figure shows that the security with varying data packets increases as the number of data packets being sent is increased by applying all the methods. However, by applying S-SOKM framework, the security achieved is comparatively high. This is because of the node's genuine nature observed through Eigen Reputation Trust management that forwards the data packet based on the reputation of the neighboring nodes, leading to minimum utilization of delay, reducing the data packet drop rate and therefore improving the security. Therefore the security is improved in S-SOKM by 11.27% compared to CKA and 22.98% compared to SPS.

4.3 Impact of data delivery ratio

Data delivery ratio is the number of delivered data packet to the destination. The data delivery ratio illustrates the amount of delivered data packets to the destination. The data delivery ratio is formulated as given below.

$$DDR = \frac{DP_r}{DP_s} * 100 \qquad (10)$$

Where 'DDR' represents the data delivery ratio that is measured using the data packets received 'DP_r' to the data packets sent 'DP_s'. It is measured in terms of percentage (%).

Table 3 Tabulation for data delivery ratio

Data Packets Sent	Data Delivery Ratio (%)		
	S-SOKM	CKA	SPS
9	75.35	64.19	54.28
18	79.14	68.10	58.04
27	84.29	73.24	64.16
36	73.14	62.10	53.04
45	78.27	67.23	56.17
54	83.14	72.10	63.04
63	85.21	75.17	64.11

To conduct experiments and analyze data delivery ratio, a network scenario with 9 data packets with an average of 763KB with each data packets holding 9KB is considered. The results observed was the data packet received using S-SOKM was 7, 6 using CKA and 5 using SPS. Table 3 shows the tabulation for data delivery ratio and the resulting graph is plotted in figure 7. Its performance increases with the increase in the number of data packets sent in the network. In figure 7 we can see that the One Hop Certificate Exchange deployed in S-SOKM framework performs better in terms of data delivery ratio compared to the other conventional methods [1] [2].

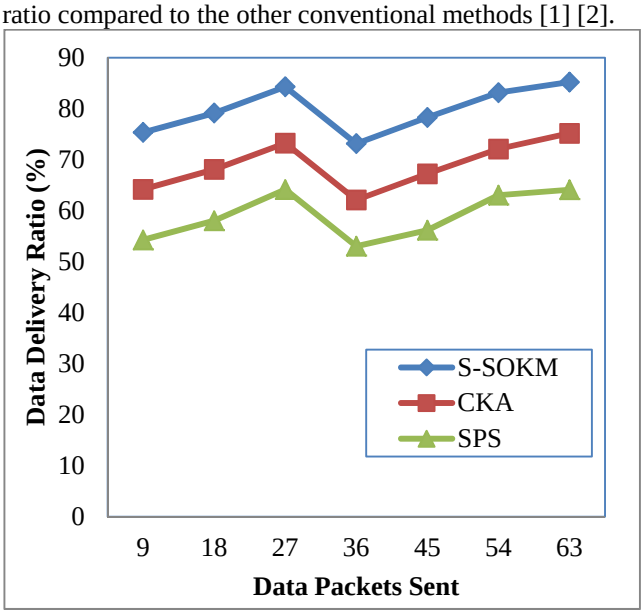

Figure 7 Measure of data delivery ratio

The results utilizing S-SOKM framework shows that using one hop certificate exchange algorithm has resulted in better data delivery ratio compared to [1] [2]. While CKA and SPS improved data delivery ratio but at the cost of security whereas, applying the one hop certificate exchange algorithm, not only the data delivery ratio is improved but at the rate of improved security. On the other hand, by applying One Hop Certificate Exchange, the confidence is measured and assigned to the certificates according to the confidence value based on the public key certificate possessed by the destination node. In figure 7, the S-SOKM framework achieves an increase of about 13.73% and 26.16% in data delivery ratio.

5. CONCLUSION

In this paper, we have proposed S-SOKM, a Secure and Self Organizing Key Management framework for MANET. S-SOKM first generates the public key certificate, with the help of a simple public key certificate validity that generates public/private keys. This analysis reveals that an optimal key certificate generation approach therefore reduces the average end to end delay required to achieve a key for each mobile nodes. The framework also examines the reputation and trust of neighboring mobile nodes, and demonstrates that with the high reputation and trust nodes, data packets are forwarded and therefore improving the rate of security. Finally, one hop certificate exchange assigns the confidence to the certificates based on the authentication through Eigen Reputation Trust Management to enhance the data delivery ratio. We demonstrate through analysis and experiments that our self organizing key management framework is effective improving the security, data delivery ratio, and imposes an average end to end delay.

REFERENCES

[1] Ning Wang, Ning Zhang, and T. Aaron Gulliver, "Cooperative Key Agreement for Wireless Networking: Key Rates and Practical Protocol Design", IEEE Transactions on Information Forensics and Security, Volume 9, Issue 2, February 2014, Pages 272-284.

[2] Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, "A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks", IEEE Transactions on Parallel and Distributed Systems, Volume 24, Issue 2, February 2013, Pages 209-224.

[3] Khaleel Mershad and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, Volume 62, Issue 2, February 2013, Pages 536-551.

[4] Haiying Shen, and Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE Transactions on Mobile Computing, Volume 12, Issue 6, June 2013, Pages 1079-1093.

[5] Junbeom Hur and Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", IEEE/ACM Transactions on Networking, Volume 22, Issue 1, February 2014, Pages 16-26.

[6] Hailun Tan, John Zic, Sanjay K. Jha, and Diethelm Ostry, "Secure Multihop Network Programming with Multiple One-Way Key Chains", IEEE Transactions on Mobile Computing, Volume 10, Issue 1, January 2011, Pages 16-31.

[7] Chan Chen, and Michael A. Jensen, "Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients", IEEE Transactions on Mobile Computing, Volume 10, Issue 2, February 2011, Pages 205-215.

[8] Tansu Alpcan, and Sonja Buchegger, "Security Games for Vehicular Networks", IEEE Transactions on Mobile Computing, Volume 10, Issue 2, February 2011, Pages 280-290.

[9] Chi Zhang, Yang Song, Yuguang Fang, and Yanchao Zhang, "On the Price of Security in Large-Scale Wireless Ad Hoc Networks", IEEE/ACM Transactions on Networking, Volume 19, Issue 2, April 2011, Pages 319-332.

[10] Jing Dong, Reza Curtmola, and Cristina Nita-Rotaru, "Secure High-Throughput Multicast Routing in Wireless Mesh Networks", IEEE Transactions on Mobile Computing, Volume 10, Issue 5, May 2011, Pages 653-668.

[11] Shengbo Yang, Chai Kiat Yeo, and Bu Sung Lee, "Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Volume 11, Issue 1, January 2012, Pages 111-124.

[12] Marco Fiore, Claudio Casetti, Carla-Fabiana Chiasserini, Panagiotis Papadimitratos, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing , Volume12, Issue 2, February 2013, Pages 289-303.

[13] Dominik Schürmann, and Stephan Sigg, "Secure communication based on ambient audio", IEEE Transactions on Mobile Computing, Volume12, Issue 2, February 2013, Pages 358-370.

[14] Albert Wasef and Xuemin (Sherman) Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks", IEEE Transactions on Mobile Computing, Volume12, Issue 1, January 2013, Pages 78-89.

[15] LinYaoa, JingDengb, JieWanga, GuoweiWu, "-CACHE:Ananchor-based public key caching scheme in large wireless networks", Elsevier, Computer Networks, Volume 87, 20 July 2015, Pages 78–88.

[16] Sukin Kang, Cheongmin Ji, andManpyo Hong, "Secure Collaborative Key Management for Dynamic Groups in Mobile Networks", Hindawi Publishing Corporation, Journal of Applied Mathematics, Volume 2014, August 2014, Pages 1-11.

[17] Yiying Zhang, Chunying Wu, Jinping Cao, and Xiangzhen Li, "A Secret Sharing-Based Key Management in Hierarchical Wireless Sensor Network", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2013, May 2013, Pages 1-8.

[18] Wei Zhang, Shanyu Tang, Liping Zhang, Zhao Ma, and Jun Song, "Chaotic Stream Cipher-Based Secure Data Communications over Intelligent Transportation Network", Hindawi Publishing Corporation, International Journal of Antennas and Propagation, Volume 2015, November 2014, Pages 1-11.

[19] Yang Yang,Yupu Hu, Chunhui Sun, Chao Lv, Leyou Zhang, "An Efficient Group Key Agreement Scheme for Mobile Ad-Hoc Networks", The International Arab Journal of Information Technology, Volume 10, Issue 1, January 2013, Pages 10-17.

[20] P. Caballero-Gil and C. Hernandez-Goya, "Efficient Public Key Certificate Management for Mobile Ad Hoc Networks", Hindawi Publishing Corporation, EURASIP Journal on Wireless Communications and Networking, Volume 2011, September 2010, Pages 1-10.