Journal of
Computational and Theoretical Nanoscience
Vol. 17, 1–7, 2020

An Implementation of Trusted Key Management Protocol (TKMP) in Wireless Network

R. Jayaprakash[1,*] and B. Radha[2]
1 Assistant Professor, NGM College, Pollachi
[1]*Research Scholar, Sree Saraswathi Thyagaraja College, Pollachi, India*
[2]*Department of IT, SKASC, Coimbatore, India*

The Trusted Key Management Protocol (TKMP) provides one of the most secure communication technologies in MANET cluster-based data protection. For security reasons, TKMP is a trusted key that can be sent to all nodes in the communication cluster. This document introduces the Trusted Key Management Protocol (TKMP) feature to improve the quality of secure communications over a cluster-based wireless network. The proposed TKMP execution process includes CBPPRS (Cluster Based Privacy Preserving Routing Selection), LBCPR (Load Balancing Cluster Based Privacy Routing) and DLBPS (Dynamic Load Balancing Privacy Path Selection) procedure. To lock the data from the malicious node, the Paillier Cryptosystem (PC) encrypts packets with homomorphic encryption. The trust score makes it easier to update routing information and improves network throughput. The experimental results show that the proposed TKMP method works better than the other Trust-ECC method.

Keywords: Cluster Network, Secured Communication, CBPPRS, LBCPR, DLBPS.

RESEARCH ARTICLE

1. INTRODUCTION

A mobile Adhoc wireless cellular network is a set of nodes connected by certain legal connections to transfer packets from one node to another [1]. There are many protocols for designing a communication structure. The direct connections are using routing protocols for the Adhoc network. There are many challenges, such as controlling mobile devices and reducing overhead when nodes have partial resources. The most important component of the protocol is to mitigate the consequences of a protocol attack. Due to the nature of the transmission network, an attacker is looking for traffic, packet loss, and hacking within the transmission range.

The literature review describes several improved routing protocols. However, some requirements of the routing protocols are contradictory. Taking the shortest path to the base station slows down intermediate nodes, which shortens the life of the network. At the same time, always choosing a shorter path reduces energy consumption and reduces network delays. Routing destinations are application specific, offering different routing systems for different applications [2]. These routing systems differ greatly in their destinations and routing methods. Most routing protocols are subject to unexpected security risks. Cluster Head (CH) attacks are primarily harmful.

The secure cluster-based MANET routing protocol is designed to protect against malicious external nodes or accessible internal MANET nodes [3]. The life of the sensor assembly largely depends on the battery life. Using WSN Multi-Bounce, each terminal is treated as a dual transmitter, an information transmitter and an information desk [4]. Failure of some of the failed sensor nodes can lead to significant topographical changes, particle rearrangement, and system improvements. Some sensor assemblies may short circuit or break due to force, physical injury or natural resistance. Fraud of sensor nodes should not affect the overall performance of the sensor system. Other ways to send information to a synchronization node or administrative base station agreement [5–6] should be considered.

In the paper, implementation of a new secure routing key management scheme based on the Trusted Key Management Protocol (TKMP) authenticates the encryption with public and private keys. At this point, the encryption and decryption algorithm is used to protect packets or messages by attackers. The following section presents current studies and ideas for common key development methods. In Section 3 we present our specific TKMP model, which introduces a new trust key model and describes the testing

*Author to whom correspondence should be addressed.

process. Section 4 describes the performance evaluation of the TKMP algorithm and finally closes the references in the last section.

2. BACKGROUND STUDY

Reference [7] examined the problem of building a new structure for the dynamic organization of mobile nodes in clustered wireless peer-to-peer networks in which Reliability in the face of topological changes must be guaranteed by the movement of the nodes, the failure of the nodes and the insertion/removal of the nodes. The main contribution of our work is a new AD HOC strategy for wireless clustering and improvements to the popular Weighted Clustering Algorithm (WCA).

Reference [8] proposed a safe and energy efficient weighted clustering algorithm (ES-WCA) for mobile WSN using a combination of five metrics . These metrics include a behavioral level metric used to ensure that the cluster leader is chosen in the sense that it will never be a malicious node.

Reference [9] proposed to use hybrid encryption using advanced encryption algorithms (AES) and elliptic curve cryptography (ECC). AES is used as a symmetric algorithm to encrypt routing information, while ECC is used as an asymmetric algorithm to encrypt the public key. During encryption, the original plaintext is converted to ciphertext using the encrypted public key, and during decryption, the ciphertext is converted to the original plaintext with the decrypted private keys. Therefore, the proposed method includes AES and ECC algorithms that provide an efficient and sufficient security mechanism.

References [10, 13] suggested that location-based routing is necessary for forwarding packets. To ensure the security of data packets, the existing algorithm has been extended to a "routing protocol that recognizes a safe location." Nodes are discovered using the clustering method. This register predicts the future location of the node by optimizing the swarm of particles. Connection time, speed, distance and node position are calculated in advance to find the best route. The node confidence value is calculated from the neighboring node. This will help predict future locations and find malicious hosts on the network to reduce packet loss. To prevent data entry from malicious hosts, packets are encrypted using elliptic curve encryption.

A network group that protects privacy. The cluster head is reliable for communication with connections in the cluster, which uses additional battery dominance (power). When evaluating cluster members in a cluster. Sending packets (message information) to and from the cluster makes it difficult to test network stability. The goal was to use Framework NS (Network Simulator) 2.34 to provide a "clustering algorithm for selecting a routing protocol to protect data in the internal and external cluster." The cluster header selection model based on routing protocol selection is entirely based on original routing and on-demand process. It was chosen as the routing protocol for triggering and testing ad-hoc transmission, which is different from on-demand messaging between mobile nodes on a convenient ad-hoc network.

Reference [11] offered an original paper on load estimation based on the Alone Privacy Routing Protocol (LBCPR) algorithm for commercial mobile networks based on connection strength and the chapter on sampling cluster with the HC-Design 2.34. Disproportionate impact of LBCPR in a group and notion or preference for centrally located data points. The predicted direction capture metric is based on cluster, weight, and minimum path to determine the path that mobile nodes will take due to the lighter weight.

(R. Jayaprakash, B. Radha, **2019**) [12] proposed a new algorithm for the Dynamic Load Balancing Privacy Path Selection (DLBPS) for cellular peer-to-peer networks based on packet forwarding and attack prevention with NS (Network Simulator) 2.34 Framework. DLBPS balances the mobile load of the gateway in the network to achieve a higher overall data rate. Meanwhile, the proposed algorithm will configure the survey, privacy manager, privacy collector, and privacy manager to complete the privacy path selection.

Trusted Key Management Protocol (TKMP) method [13], in which the exchange of trusted keys for all cluster nodes is computed during data exchange for security reasons. TKMP assigns the value of a dynamic exchange of public and private keys to a trusted variable that is checked during communication. For example, the proposed complete protocol is implemented in three phases such as Initial distribution, key generation, key verification and validation.

3. IMPLEMENTATION OF TRUSTED KEY MANAGEMENT PROTOCOL (TKMP)

TKMP enables the selection process for Cluster Based Privacy Preserving Routing Selection (CBPPRS), Load Balancing Cluster Based Privacy Routing (LBCPR) and Dynamic Load Balancing Privacy Path Selection (DLBPS). We have already presented the complete proposed TKMP system, as shown in Figure 1 (R. Jayaprakash, B. Radha, 2019). This implementation consists of three phases: CBPPRS, LBCRP and DLBPS. In the first phase, the CBPPRS routing selection algorithm for adhoc mobile networks is used based on the strength of the connection and the selection of the cluster header. In the second stage, the load imbalance in the LBCPR network also leads to a bias or bias in the selection of nodes that are centrally located for data transmission. The DLBPS method compensates for the mobility of the gateway on the network in order to achieve a higher data rate after loading. Finally, TKMP improves the quality of secure communication in wireless cluster networks.

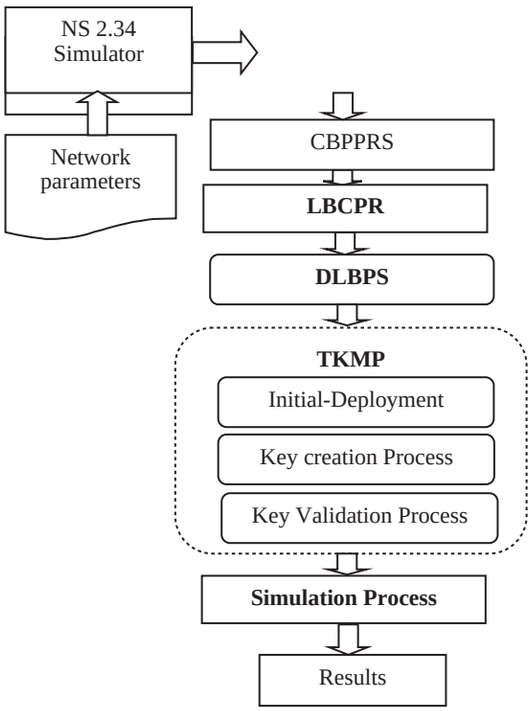

Fig. 1. TKMP process flow.

3.1. Network Architecture

Network architecture consists of *M* number of nodes that are randomly distributed in network modeling. Some nodes in this architecture are arranged in clusters. We have already presented an assessment of the formation of a network in a graphical model [11]. The network architecture model is shown in Figure 2.

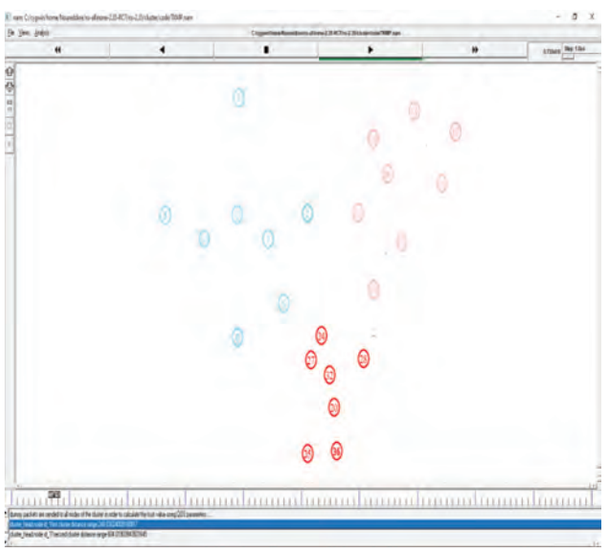

Fig. 2. Network architecture.

Fig. 3. Cluster head (CH) assignment.

3.2. Cluster Based Privacy Preserving Routing Selection (CBPPRS)

Cluster Based Privacy Preserving Routing Selection (CBPPRS) has already been implemented [11] and plans to collect cluster heads (CH) based on network power consumption. This method creates a link generation model for each link generation to select CH and determines the model with the highest revision interval (link generation) for the cluster header to identify a cluster update. The cluster header life time when a cluster header is selected from a node location, the node location becomes normal. Figures 3 and 4 show the starting position of the CH and the assignment of the node ID.

3.3. Load Balancing Cluster Based Privacy Routing (LBCPR)

We have already introduced LBCPR (Load Balancing Cluster Based Privacy Routing) to unbalance the network

Fig. 4. Nodes ID, CH and base station (BS) position.

RESEARCH ARTICLE

Fig. 5. LBCPR energy level utilization.

load [11]. In this process the strength of the bond and the formation of the selection of the cluster head are identified. LBCPR search links and response algorithms measure the charge between all possible neighbors using possible energy. At the same time, this method improves the performance of the hubs against load imbalance and ensures the reliability of the connected subnets. Figure 5 shows the LBCPR process.

Fig. 6. Source and destination node assignment.

Fig. 7. Packet transmission using privacy path selection through cluster one to another cluster.

Fig. 8. Packets received without Key assignment through cluster one to another cluster.

3.4. Dynamic Load Balancing Privacy Path Selection (DLBPS)

We have already provided options for Dynamic Load Balancing Privacy Path Selection (DLBPS) [11]. This method searches for continuous paths to send packets from source to destination via the cluster head with the selected base station. At this point, this method balances the mobile load of the gateway on the network and achieves greater overall data performance. DLBPS is not a secure communication channel on a cluster network. To overcome this problem, the Trusted Key Management Protocol (TKMP) was introduced, which creates a secure communication channel on the cluster network, which is described in the next section.

In Figures 7 and 8 above, the source node 10 sends a packet to the destination node 25. The source and destination nodes are on nodes 1 and 20 with different clusters.

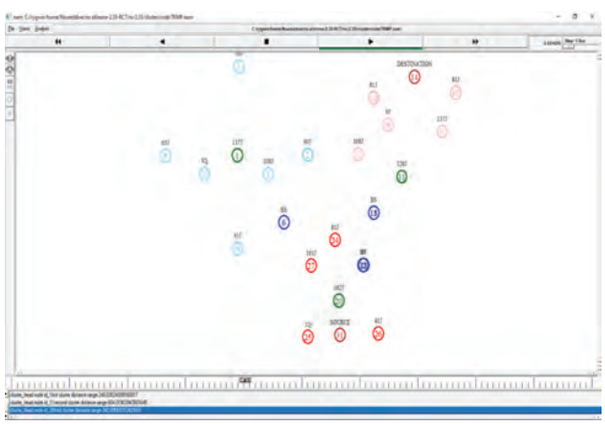

Fig. 9. Source and destination node assignment.

RESEARCH ARTICLE

Fig. 10. Packet transmission using TKMP Privacy Path selection through cluster one to another cluster.

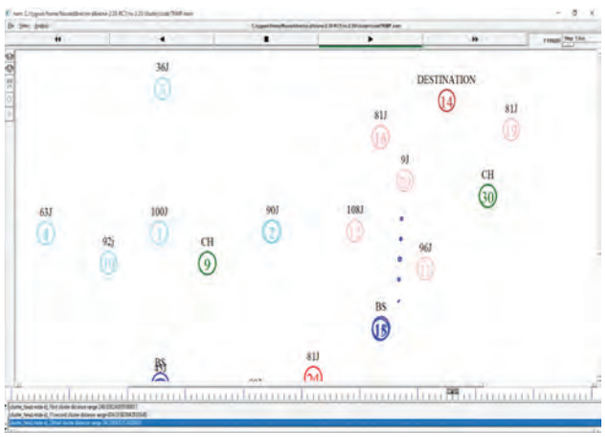

Fig. 11. Packet transmission with packet drop through cluster one to another cluster.

Source Node CH Node 1 sends packets through a Base Station (BS) node 6, the CH node 20 and finally the packets of the destination node 25.

3.5. Trusted Key Management Protocol (TKMP)

The Trusted Key Management Protocol (TKMP) we have already introduced (R. Jayaprakash, B. Radha, 2019) undergoes major development in three specific phases: (a) Initial installation, (b) Key generation, and (c) Confirmation basis and validation. The TKMP method can be considered as an evolution of the Paillier encryption system

Table I. Simulation parameters.

Parameters	Symbol	Value
Mobile nodes	MN	5–50 in steps of 10
Simulation area	Row × Column	1000 × 1000
Transmission range	TR	5–50 in steps of 10
Routing protocol	CBRP	CBRP
Node energy	E_{node}	100 Joules
Boosting energy	E_{boost}	100 J/bit/m^2

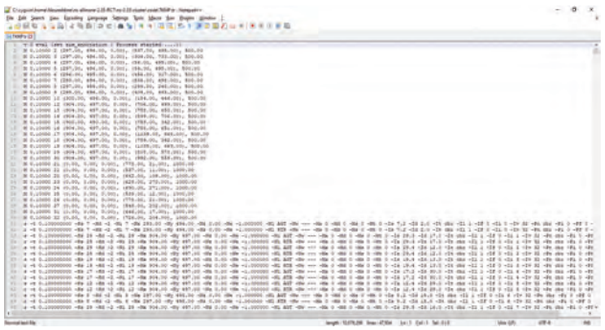

Fig. 12. TKMP trace file.

that uses the public key for secure communication. This method implements the homomorphic encryption of the Paillier cryptosystem (PC) using the encryption key. It also creates a mathematical model developed using advanced components such as hash function, homomorphic encoding, profile typing, and secure data transfer random number functions. Figure 9 describes the source destination nodes for transferring packets via TKMP.

In Figure 10, the node 29 has less energy than 9 joules, so the entire envelope is discarded during the specific node transfer.

4. PERFORMANCE EVALUATION

The performance of the proposed TKMP system takes into regard as 50 to 200 nodes in the mobile adhoc network and

Table II. Comparison of packet delivery ratio with existing trust-ECC with proposed LBCPR, DLBPS and TKMP algorithm.

Number of nodes/system	50	100	150	200
Trust-ECC	98.25	91.5	88.23	85.99
LBCPR	98.85	92.22	89.63	86.38
DLBPS	99.02	93.47	90.09	87.88
TKMP	**99.82**	**95.17**	**93.81**	**88.72**

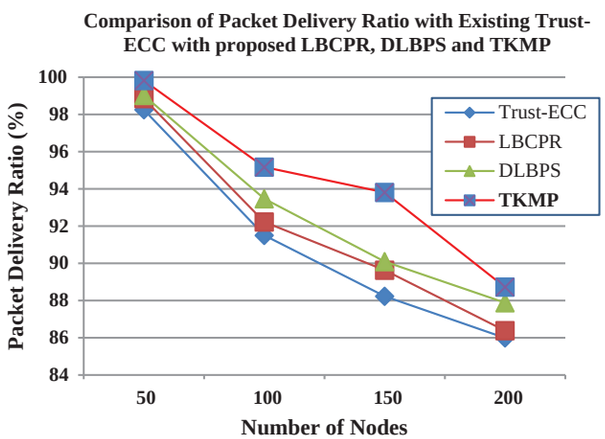

Fig. 13. Chart of packet delivery ratio.

RESEARCH ARTICLE

Table III. Comparison of throughput ratio with existing trust-ECC and proposed LBCPR, DLBPS and TKMP.

Number of nodes/system	50	100	150	200
Trust-ECC	25.5	26.8	19.5	17.5
LBCPR	25.7	25.9	20.11	16.8
DLBPS	24.47	25.18	19.06	15.33
TKMP	**23.39**	**24.16**	**18.82**	**14.08**

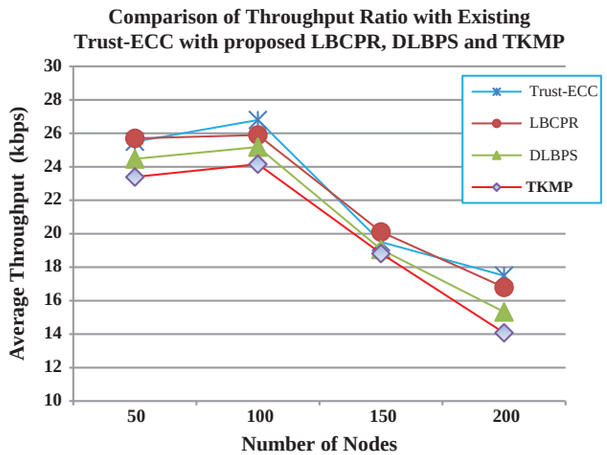

Fig. 14. Chart of throughput.

Table IV. Comparison of delay ratio with existing trust-ECC and proposed TKMP.

Number of nodes/system	50	100	150	200
Trust-ECC	0.35	2.42	5.8	8.6
LBCPR	0.34	2.38	5.1	7.8
DLBPS	0.32	2.19	4.86	7.2
TKMP	**0.29**	**2.01**	**4.20**	**6.7**

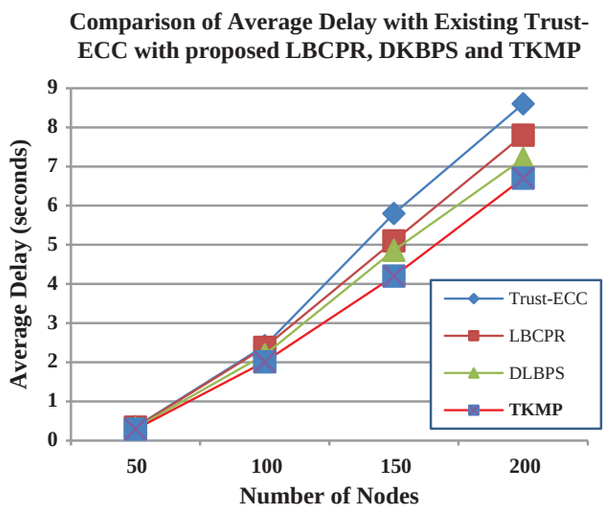

Fig. 15. Chart of packet delay ratio.

the nodes are used in an area between 1000 m × 1000 m. The simulation parameters are shown below.

The Packet delivery ratio (PDR) is defined as the portion of the package shipped that is normally interchangeable between all packages shipped through the destination. The proposed TKMP algorithm offers a better PDR ratio than the proposed trusted ECC system [13].

The comparison of TKMP performance is shown in Figure 13, which shows the performance of the existing Trust-ECC funding system [13].

The proposed TKMP algorithm has a higher average latency than the Trust-ECC system [13].

5. CONCLUSION

The main objective of this document is to improve the quality of secure communication over cluster-based wireless networks using the Trusted Key Management Protocol (TKMP). The specific TKMP method follows the selection of CBPPRS (Cluster Based Privacy Preserving Routing Selection), LBCPR (Load Balancing Cluster Based Privacy Routing) and DLBPS (Dynamic Load Balancing Privacy Path Selection). The experimental results show that the specific TKMP method performs better than the current Trust-ECC method. At the same time, the proposed algorithm creates a developed geometric model using secure elements such as hash function, homomorphic encryption, profile key sequence and random number functions for secure data transmission.

References

1. Shanmugapriyan, D. and Murugaanandam, S., **2014**. Secured and highly reliable data transfer in MANET using position-based opportunistic routing protocol. *International Journal of Innovations in Scientific and Engineering Research, 1*(2), pp.69–74.
2. Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C. and Belding-Royer, E.M., **2002**. A Secure Routing Protocol for ad hoc Networks. *IEEE International Conference on Network Protocols*, Paris, France, pp.78–87.
3. Azarderakhsh, R., Reyhani-Masoleh, A. and Zine-Eddine, A., **2008**. A Key Management Scheme for Cluster Based Wireless Sensor Networks. *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Vol. 2, pp.222–227.
4. Udaya, D., Suriya, Rajkumar, Rajamani and Vayanaperumal, **2013**. A leader based monitoring approach for sinkhole attack in wireless sensor network. *Journal Computer Science, 9*(9), pp.1106–1116.
5. Xun, Y., Russell, P. and Elisa, B., **2014**. Homomorphic encryption and applications. *Springer Briefs in Computer Science*.
6. Jiang, Q., Zeadally, S., Ma, J. and He, D. **2017**. Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access, 5*, pp.3376–3392.
7. Aissa, M., Belghith, A. and Drira, K., **2013**. New strategies and extensions in weighted clustering algorithms for mobile ad hoc networks. *Procedia Computer Science, 19*, pp.297–304.
8. Amine, D., Nassreddine, B. and Bouabdellah, K., **2014**. Energy efficient and safe weighted clustering algorithm for mobile wireless sensor networks. *Procedia Computer Science, 34*, pp.63–70.
9. Sivamurugan, D. and Raja, L., **2017**. Secure routing in MANET using hybrid cryptography. *International Journal Research Granthaalayah, 5*(4), pp.83–91.

RESEARCH ARTICLE

10. Jayaprakash, R. and Radha, B., **2017**. Routing protocols and privacy preserving cluster based protocols in wireless networks: A technical review. *International Journal of Advanced Research in Science and Engineering, 6*(12), pp.1325–1333.
11. Jayaprakash, R. and Radha, B., **2018**. CBPPRS: Cluster based privacy preserving routing selection in wireless networks. *International Journal of Engineering & Technology, 7*(3.12), pp.439–443.
12. Jayaprakash, R. and Radha, B., **2020**. A Trusted Key Management Protocol (TKMP) for Cluster Based Wireless Networks. *Interational Conference on Recent Challenges in Engineering and Technology*.
13. Syed Jamaesha, S. and Bhavani, S., **2018**. A secure and efficient cluster based location aware routing protocol in MANET. *Cluster Computing, 22*(2).

Received: 3 August 2020. Accepted: 26 August 2020.