International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 27, No. 5, October, 2022, pp. 757-765
Journal homepage: http://iieta.org/journals/isi

A Neighbor Trust Weight Based Cryptography for Multi Key Distribution for Improving Quality of Service in MANETS

Rajesh Yamparala[1,2*], Sankara Narayanan Selvaraj Pandian[1]

[1] Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-600062, Tamil Nadu, India
[2] Department of CSE, Vignan's Nirula Institute of Technology & Science for Women, Guntur, Andhra Pradesh 522009, India

Corresponding Author Email: rajeshyamparala@gmail.com

https://doi.org/10.18280/isi.270508

Received: 10 July 2022
Accepted: 6 October 2022

Keywords:
routing information, multi key generation, identity with trust level cryptography, key generation, key distribution, network security, trusted node, network performance

ABSTRACT

A Mobile Ad-Hoc Network (MANET) is a self-configuring network that provides temporary connections to several wireless nodes. Trust mechanisms are employed in routing protocols to quickly locate a safe path. Because of its openness and complexity, MANET can be attacked in a number of ways. To begin mitigating potential security risks, a number of different cryptographic key generation strategies are explored. A key management system for MANET security is available with different encryption techniques. Identity with Trust Level based Cryptography Model (ITLCM) is used to generate multiple keys and distribute these to particular targets. At this stage, key management protocols are essential to any secure group architecture of communication. Because of its dynamic topology which extensively affects its application, the multi key management is an essential task. When compared to more conventional methods of protecting a network, MANET security is entirely novel. Security routing protocol implementation is difficult since it requires the production and distribution of multiple keys. To provide both connection and message protection without relying on third parties, the Neighbor Trust Weight based Routing Model (NTWRM) is designed. In the proposed model, a trusted node is selected to monitor all of the nodes in the routing process to create a stable multi-key distribution environment that enhances MANET performance. In comparison with traditional methods, the proposed model shows that its findings are better than the existing ones.

1. INTRODUCTION

A decentralised MANET is used to construct a dynamic network where there is no central authority and no permanent infrastructure [1]. They communicate with one another in a multi-hop fashion to get past contact coverage and resource limitations [2]. Based on their relative proximity, nodes either make direct connections to one another or act as hosts and routers [3]. Node-to-node data transfer is essential to a functional network. MANETs are especially vulnerable to routing attacks from within the network due to their open topology, decentralised structure [4], and absence of a central authority. This makes complicated network routing a challenging problem in general. Multiple routing assaults [5] are not prevented by the standard approaches to routing in ad hoc networks [6].

External attacks are typically resisted using security schemes due to traditional cryptographic systems. They are, however, ineffective in defending against attacks initiated by internal malevolent nodes [7]. By engaging in various types of packet-forwarding misbehaviors, such malicious nodes can have a significant impact on network security [8]. In such a hostile environment, incorporating the principle of "confidence" and "trust" would allow for forecasting of neighbor node activity [9]. The principle of trust may be useful in competitive environments where nodes would rely on one another to achieve their objectives securely. Trust supervision arrangements have recently been proposed as a feasible security solution for improving MANET routing resolutions by detecting malicious nodes [10].

The acronym ADMA stands for an Autonomous Decentralized Management Architecture [11] that was developed to bring autonomic concepts to MANETs. This feature enables the network to automatically adapt to new conditions without requiring manual intervention [12]. Our system is decentralised and runs in a peer-to-peer fashion, so it doesn't need a central authority to manage the network [13]. With the help of monitoring data and preset high-level policies [14], every mobile node that uses ADMA components can make the right call at the right time [15].

Ad hoc nodes in MANETs independently relay information and command packets they have received from other nodes. Therefore, rogue nodes pose a significant security risk and make it challenging to secure the MANET [16]. This is due to the fact that packet content collected from other nodes is not guaranteed and may be altered or discarded. When it comes to raising Quality of Service (QoS) [17], the routing protocol plays a crucial role. Disruptions to data transmission can occur in MANETs due to the chaotic topology and autonomous behaviour of their nodes [18]. This phenomenon requires a protocol to route to the destination that will find more secure and skilled routes. Routing protocols are ongoing research aimed at enhancing MANET's security by developing current security systems or proposing new securities [19]. This means that the efficiency and protection of a MANET have to be resolved. The common attacks in MANETs include the loss of packets [20], malicious node injection with fake route information, excluding target node from routing or routing requests attacking the target node [21]. These scenarios trigger inefficient routing and degrade network efficiency. The structure of MANET is depicted in Figure 1.

Figure 1. MANET structure

MANET has a great deal of functionality left to offer as compared to traditional networks such as ARPANETs [22]. This system is insecure because it is vulnerable to both passive and active attacks as well as having a public feature [23]. There are more group problems that remain in MANETs, relative to point-to-to-point systems [24]. The scheme gets inappropriate details to the members of the community and they must keep the content's integrity. Multicast data can be encrypted using a group key [25]. A dynamic group membership is required to allocate the latest key to each member [26]. The main drawbacks of the existing model sis that they are vulnerable to attacks that need to be reduced with the trusted key distribution model for enhanced quality of service [27].

1.1 Key distribution

In mobile ad hoc networks, many modern technologies include group-oriented communication. Multicast is an effective way to support group-oriented applications, particularly with a limited bandwidth and power in the mobile environment. It is necessary to provide secure multicast communication if such applications are to be used in a conflicting environment. The main obstacle for safe multicast communications is key management. The challenging factor of "1 affects n" must be resolved by the multicast key distribution [28]. Multi-cast communications with secure key distribution relies heavily on security services include authentication, data integrity, access control, and group confidentiality. Privacy within the community is the most important backbone for many apps. Sharing a secret enables this security function, but doing so securely is the primary problem of key management in designing secure multi-cast and efficient community systems of communication.

Most of these security services typically rely on coding using traffic coders and coding uses coding keys. Key management involves the development, distribution and update of keys, which is a basic block for stable multi-level applications. Each member holds a key to encrypting and decrypting the multicast data in a secure multicast communication. In order to fulfil the multicast key management criteria, a member must update and distribute to all members when they leave the group.

Encrypting and authenticating data exchanged between nodes in an ad hoc network is crucial to ensuring the privacy of communications. For these security processes to go smoothly, it's important that users agree on a shared set of keys beforehand. Ad hoc mobile network key distribution is made more difficult by MANET constraints than it would be in more traditional networks. Traditional key distribution systems rely on a Certificate Authority (CA) or Trusted Third Party (TTP) to issue users with certificates that may be used to verify the authenticity of public keys. In order to ensure safe communication, the suggested model employs an efficient routing model, and to boost the system's performance, it uses an efficient key distribution model. The introduction section discuss about the MANET routing and quality of service models. Section 2 discuss about the literature review of the traditional models, section 3 discuss about the proposed model for routing and trust level based cryptography model. Section 4 discuss about the results and section 5 concludes the paper.

2. LITERATURE SURVEY

A trust management system for MANETs was developed by Xia et al. [1]. Accurate packet forwarding rates, rather than source and destination IP addresses, are used to establish trust between surrounding nodes. It's another name for fuzzy trust, and it takes into account a node's viewpoint, its current abilities, and the amount of work it has done in the past to arrive at an estimate of its current trust. Nodes of bad behaviour are foreseen by this study. When selecting such a path, it is common practice to bypass potentially dangerous intermediate nodes. When cooperation or collaboration is essential to achieve mission and system goals like dependability, availability, scalability, and reconfigurability, trust management in a dispersed Mobile Ad Hoc Network (MANET) becomes a significant challenge. Defining and managing trust in a military MANET necessitates taking into account the interactions between both composite cognitive, social, information, and communication networks, as well as the severe resource constraints, and the dynamics of the system. We aim to establish a composite trust measure by combining the concepts of "social trust," gleaned from social networks, and QoS trust, gleaned from communication and information networks. Using societal conceptions of trust, we explore its concepts and attributes and deduce some distinctive features of trust in MANETs.

According to Gharehkoolchian et al. [2], to mitigate node corruption, they introduced a new trust model that incorporates TLs for nodes and sets limitations on TL level. For every node in the network, a TL is assigned It is said to be more respectable if it generally functions by distributing packets and is given the IP address 2. TL is set to 0 to denote the case of potentially malicious activity TL is set to −1 is allocated if the node is found to be three times likely to be malicious. In route discovery, the TL value of a node's neighbors is examined. If the response is correct, it is sent (Route 2). If a request has not been seen previously, the request will be returned to the suspicious node (TL=1). When the suspect node sends an odd reply, the route reply is discarded.

In order to reduce needless routing calculations and facilitate fast communication, remove superfluous routing logic and tracking details Airehrour et al. [3] proposed the

Grade Trust Protocol to identify and distinguish adversaries that give low scores. Nodes are categorized according to the degree of confidence, based on a scale that runs from "trusted" to "mates", "m" friends, and "potential" friends. The trust level is calculated by dividing the number of monitoring packets received by the number sent packets. When the packet is presented to a trusted neighbor of Tr, the packet hops to the following node, which decides which destination to use based on the result of the evaluation from Trusted Friends. In the absence of a mate, a friend is selected. A less secure node is transferred to a lower level of trust rapidly. This disadvantage notwithstanding, the trust system does not account for the forwarding ratio, which leaves them open to packet loss.

Patel et al. [4] suggested a trusted model for MANETs in which energy consumption is the same for every node. A trust rating is assigned based on metrics such as how long it takes for ratios to drop, how long control has been disabled, and how much power is left in the system. The model tried to find a secure the end-to-end route the trust of the neighbor. The new path would have the highest value of routes, much like the existing path, and is equal to all other paths that it gets. Since data may be resent in the event of packet loss, the scheme does not provide a self-recovering defense mechanism during transmission.

Highlighted two ways to determine trustworthiness: trust control, and trust validation, illustrated in the work of Gupta et al. [5]. Aggressive or nonaggressive nodes may be used as trust monitors. Indirect information, such as peer node ideas, is essential to transmit trust information. In general, Nodes may use data, such as identifiers, public keys, or addresses as evidence of confidence [6]. Mandhare et al. [7] developed an attack-shielding strategy known as the target management framework. In most MANETs [8], a combination of trust ties between nodes is employed to maintain trust [9] and the trust ties among the nodes is achieved through OTS [10].

Hemalatha et al. [10] have detailed the procedure for treating greyholes in the MANET network attack in the research methodology. For measuring people's willingness to take risks, they tested and gave recommendations. Because of its high trust levels, the source node is likely to be able to select several routes to the destination. To find an authorized and reliable path, a source begins broadcasting packages to its neighbors to try to identify an alternative route. Insecure locks can be avoided by taking advantage of the GKEY certificate when possible. The Secure Lock proposed by Mohammadani et al. [11] utilizes one-registration protocol in which the key server needs to broadcast only in the event of the network node leaving or all nodes have to be re-registered. This protocol does away with re-key messages at the very source. However, since all of the messages have been sent to the third party, the calculation of Chinese Remainder remains the same in the cloud model.

Moudni et al. [12] designed a key management scheme which ensures the true nature of a distributed network. Ad-hoc mobile networks that involve sensor nodes with reduced computing and communication capabilities are Distributed Sensor Networks (DSNs). A key management system presented will satisfy the organizational and security requirements of DSNs [13]. In addition, their scheme includes the selective distribution and repeal of sensor node keys and re-keeping of nodes without significant calculation and communication capabilities.

The contribution of group key management protocol was suggested by Singh et al. [14] in order to secure data traffic among group members. It is called as the Chinese theorem with differential approach, which focuses on ensuring reliable contact between members of the community. The contribution means that each member's share community key that is determined by collecting those members' for sharing. A few rounds are needed to calculate the share key for this protocol. The main calculation is performed in parallel with all group members. The central administrator or server would not rely.

Jain et al. [15] have suggested an effective key management protocol for MANET. Here, due to a node exit or node entry, the priority provided to the processing of complex structural changes enters the network. All members are divided into clusters to manage the complex structural changes. Singh et al. [16] suggested a MANET environment with main public group management approach based on network nodes' composite trust level. In this model, the nodes take big decisions, for example routing, through trust levels. The trust levels for any node verifies the 4 constraints: (1) the node can decide to continue communicating with other nodes; (2) the threshold value of the node can be set to deal with risk evaluation; (3) the reliability is observed as the opinion of an adjacent node's behavior; (4) every individual can experience the behavior of the adjacent nodes over a period of time.

3. PROPOSED MODEL

On any mobile host, a routing protocol is implemented and is thus restricted to each node by resources. Therefore, an effective routing strategy is desirable in order to guarantee connectivity so that nodes can communicate quickly. This routing strategy must minimize the overload of computation on mobile host and network traffic. The following are assumed from the proposed Trust Level based Cryptography Model (ITLCM) and Neighbor Trust Weight based Routing Model (NTWRM) scheme:

- ➢ All mobile nodes have the same physical features.
- ➢ Network wireless connections are two-way.
- ➢ All nodes run in a Secret Auditor Mode (SAM) in order to observe neighboring nodes and their behavior.
- ➢ A central auditor node (CAN) is selected from the network to monitor all nodes for their trust factors.
- ➢ A cryptography model is used for generation of keys for identification of trusted nodes.

The proposed trust model uses shortest observations to derive neighboring node mistrust by analyzing neighbor nodes packet falling ratios, energy consumption ratios. Furthermore, each node uses a discovery mechanism for attack patterns that detects nodes that are malicious. Recommendations from trusted neighbors to enhance routing decisions are also considered. The CAN is selected based on the computational capabilities, trust factors, energy consumption levels and neighbor feedback rate.

3.1 Neighbor trust weight based routing model (NTWRM)

In the proposed routing method when a network is established, the CAN node is selected and then it calculates the trust factors of all nodes. The nodes whose trust factors are more than the threshold can be considered to involve in routing. The trust factor of each node is calculated as:

$$T_R = \sqrt[n]{\prod_{i=1}^{n} T_{i,j}, node_i \; and \; node_j} \in route \sum_{i=1} Max(PDR(i)) + Th$$

$$R \; and \; node_i \rightarrow node_j, i \neq j$$

$$TL = \left(1 - \frac{n}{N}\right) \times T_R > Th, \qquad n = CAN_{Ns} + N_{is}$$

The sender determines the mistrust of the neighbor node by monitoring neighbor's behavior. In particular, if N_J does not forward packets sent by N_i, the node N_i will increase the discrepancy score of its neighboring node so that in further communications, this node will not be allowed to involve in communication. In the proposed routing mode, the values of mistrust are limited between 0 and 1 i.e, 0 for high malicious and 1 for malicious. In the proposed routing model, initially the nodes want to communicate initialize the routing process.

The CAN node is selected and then trust factors are calculated. The nodes with trust factor more than threshold value is considered. The sender will send a RACK to all the valid neighbors by checking their trust factors. The neighbor nodes will acknowledge the sender node only after taking information from the CAN node that the sender is a trusted node. The CAN node will generate keys and distribute them to the nodes involved in communication. The nodes will send their keys to the sender back as an acknowledgement.

The sender will establish the route by considering the acknowledgement key from the neighbor nodes and verifies it from the CAN node and then only updates the routing table. All the available routes from the sender to destination is recorded in the CAN node and only one shortest route is selected. The remaining routes can be used if there is any problem with the considered route. The process is continued till the route toward the destination is completed and the routing table is finalized by the CAN node. The routing process is depicted in Figure 2.

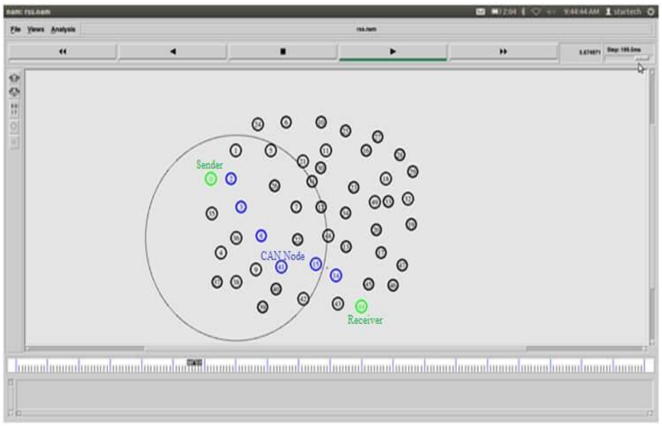


Figure 2. Routing process in proposed model

The node which transmits a packet will check within its coverage that the neighbour transmits a packet within a certain time frame to another node. Otherwise, the value assigned to the neighbour will be reduced and the packet resend instruction is forwarded by the CAN node. The CAN will continuously monitor all the nodes. When the communication is initiated, the Secret Auditor Mode is activated and each node is monitored by its neighbor node and also by CAN node and its trust factor is updated by the CAN node if any malicious behavior is observed. A SAM is used to ensure its neighbour sends the packet to the next hop in the routing table and any intermediate nodes along the way. If the nearby node does not forward the packet in the next hop to the required node, the trust factor of it will be updated by the CAN node. The route selection process is indicated in Figure 3. The packet stays in the buffer of the node, and is then removed from the buffer until transmitted successfully. The trust factor is updated as:

$$Tf_n = \sum_{i=1}^{n} tr_i \times D_Y^{X_i}, \quad W(N)_i = \frac{\frac{1}{PDR_{X_i}}}{\sum_{j=1}^{n} \frac{1}{PLR_{X_j}}}, \sum_{i=1}^{n} W_i > Th$$

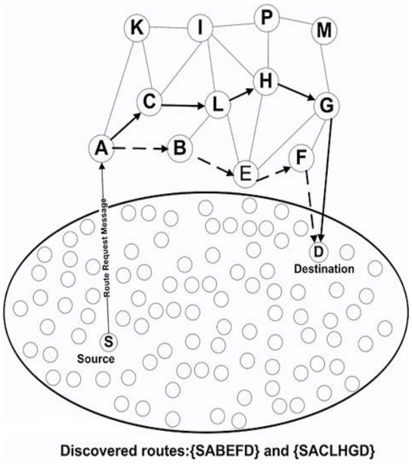


Figure 3. Route selection procedure

The route trust is also calculated and updated to the CAN node. All the available routes trust factors are calculated and then the highest average trust factor route is considered for communication. The routes trust factors are calculated as:

$$RouTr_{i,j}(t) = \frac{\Sigma_{i=0}^{N} T(i) \times T_n(i+1)}{\Sigma_{i=0}^{N} Tf(i)} > Threshold$$

The routes at the CAN node will be updated when the trust factors are updated. The most trusted route is selected for the communication. The route updating is performed as:

$$RouTu(Tf_{ij}) = RouTr(N(i)) \Big/ \sum_{i=1}^{N} Tf_{ij},$$

$$Tf_{ij} = \frac{N(i)_{ij}^{i+1} - \min\left\{N(i)_{ij}^{j}\right\}}{\max\limits_{i}\left\{N(j+1)_{ij}^{i}\right\} - \min\limits_{j}\left\{N(j)_{ij}^{j}\right\}} + Th$$

Algorithm NTWRM

```
{
Step-1: Create a network with the required nodes to initiate data communication.
Step-2: Calculate the trust factors for each and every node.
Step-3: Identify the node whose trust factor, computational capabilities and energy levels are high and consider it a CAN Node.
Step-4: Activate Secret Auditor Mode
```

Step-5: The sender will initiate the route identification process by sending RACK to all the trusted neighbor nodes.
Step-6: The neighbor nodes will verify the acknowledgement by considering the information from the CAN node and checks whether CAN node is original or not.
Step-7: The CAN node will generate the keys and distribute to all the trusted neighbor nodes.
Step-8: The neighbor nodes will send keys to the sender as return acknowledgement and the sender verifies the keys from the CAN node.
Step-9: The shortest route having high trust factor is updated in the routing table and the communication is initiated.
Step-10: After communication is completed, deactivate the Secret Auditor Mode.
}

3.2 Trust level based cryptography model (ITLCM)

In the process of routing, the proposed model considers keys for node validation. The keys are calculated using the CAN node. In the proposed work, a Trust Level based Cryptography Model (ITLCM) is introduced that calculates the keys based on the trust levels of the nodes. The keys generated are maintained by the CAN node and these keys are distributed the trusted nodes involved in the communication. The keys once shared will be erased after they are utilized by the nodes for verification. This erasing operation is performed to avoid masquerade attacks in the network. The proposed model generates multiple keys for the nodes involved in communication. The keys once used will not be reused in the proposed model. The keys generated must be unique and security need to be strictly maintained to improve the system performance.

3.3 Key generation process

MANETs are vulnerable to attack because they use wireless connections. Eavesdroppers may gain access to sensitive information for providing network security. Hackers can target the network directly to delete messages, insert false messages, or impersonate a node, violating availability, credibility, authentication, and non-repudiation. Inside a network, compromised nodes may also initiate attacks. A cryptographic key must be exchanged by all authorized network members for safe data communication. When current group members leave the system or new members join the network, this hidden key should be changed. The process of key generation is discussed briefly.

The CAN node will generate the unique keys for all the trusted nodes in the network. Based on the trusted factor of a node, the keys are generated for each node separately.

The keys for a node is generated by the CAN node by considering the two random polynomials where one is prime and other one is a random number that is greater than first polynomial.

The two numbers are considered randomly and considered as:

$$PP_i(N(i))), PPj(N(i+1)) \in N(ID),$$
$$\text{where} PPj(N(i+1)) > PP_i(N(i)))$$

The two polynomials calculate their values as:

$$PP_i(N(i))) = \sum_{i=0}^{N} Th + N(i)_{i,j} Tr^{N} \; and$$

$$PP_j(N(i+1)) = \sum_{i=0}^{N} PPi(N(i)) + Th + Tf_{i,j} Tr^{N-1}$$

$$\mathrm{Ik}(\mathrm{N(i)}) = (\mathrm{K}_{\mathrm{N(i)}} \oplus \mathrm{Rid}) \oplus (\mathrm{K}_{\mathrm{N(i+1)}} \oplus \mathrm{Rid})$$
$$\oplus \mathrm{Th} \,\&\, \mathrm{Tf}(\mathrm{N(i)}) \oplus \mathrm{PP}_{\mathrm{i}}(\mathrm{N(i)})$$

here, Ik is the intermediate key, KN(i) is the key for node I, initially it is the node id and Rid is the Receiver node ID and Th is threshold value and Tf(N(i)) is the trust factor of the node.

$$\mathrm{Ik}(\mathrm{N(i)}) = \mathrm{Ik}(\mathrm{N(i)}) \oplus \mathrm{CAN(ID)}$$
$$\oplus \left\{ {}_{\mathrm{Tf\,(Dest)}} \oplus {}_{\mathrm{Tf\,(Sender)}} \right\} \oplus \mathrm{Th} \oplus \mathrm{PP}_{\mathrm{j}}(\mathrm{N(i+1)})$$

The final key for each node is calculated as:

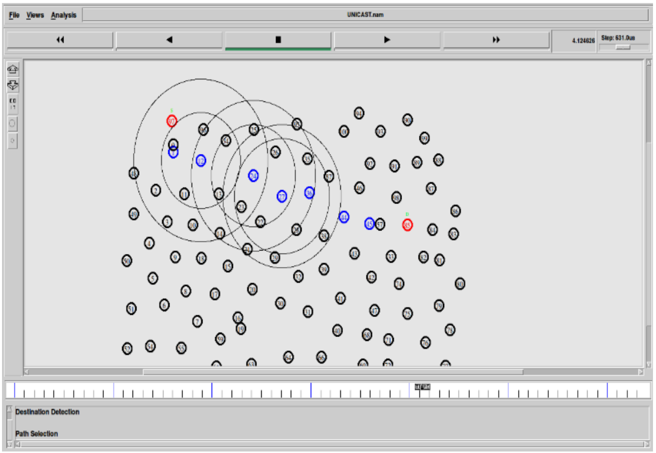
$$\mathrm{Fk(N(i)} = \mathrm{Ik(n(i))} \oplus \mathrm{CAN(ID)} \oplus \mathrm{PP_i(N(i))}$$
$$\oplus \mathrm{PP_j(N(i+1))} + \mathrm{Routr(N(ID))}$$

For authentication, all of the keys produced are used. Authentication allows a mobile node to verify the identity of the peer node with which it is communicating, preventing an attacker from impersonating a node and obtaining unauthorized access to resources and sensitive data. The proposed model performs the process of routing effectively by using the keys for authentication that improves the security levels of the system.

4. RESULTS

Table 1. MANET parameters

Parameter	Value
Coverage Area	1000 X 1000 m
MAC layer protocol	IEEE So2.00
Channel bandwidth	2 Mbps
Packet size	512 Bytes
Number of nodes	50
Pause time	5 c
Routing protocol	AODV
Percentage of malicious nodes	0-40%



Destination Detection

Path Selection

Figure 4. MANET structure

The proposed model is implemented in NS2.35 by creating a network with multiple nodes and establish a secured route by considering only trusted nodes and performing key distributions among them. MANET is a mobile device array, known as nodes, which communicate without the use of any facilities such as access points and base stations. These networks configure themselves and are able to operate themselves and can be easily deployed; hence, they are called self-organizing networks. The n odes run without centralized administration and provide connectivity. The proposed model considers the parameters that are depicted in Table 1. The proposed Trust Level based Cryptography Model (ITLCM) and Neighbor Trust Weight based Routing Model (NTWRM) are compared with the existing Trust based secured routing (TSR) model and Quantum key distribution (QKD) models and the results are evaluated based on the parameters like Routing Process Time Levels, Trust Level Calculation Time Levels, Route Security Level, Key Generation Time Levels, Key Distribution Time Levels, Packet Delivery Ratio, Packet Loss Ratio and End to End Delay.

Additional issues and problems as opposed to routing inside the wired network with a fixed infrastructure are faced by mobile ad hoc network. The mobile ad hoc network structure is shown in the Figure 4.

In this paper a highly reliable and efficient route system that not only meets the confidentiality, protection, authentication, non-repudiation, and unforgeability for ad-hoc networks, but also fulfils other required properties, such as privacy, track ability and multipath versatility, so that the ad-hoc set-up is protected. The Figure 5 depicts the Routing Process time levels of the proposed and traditional models.

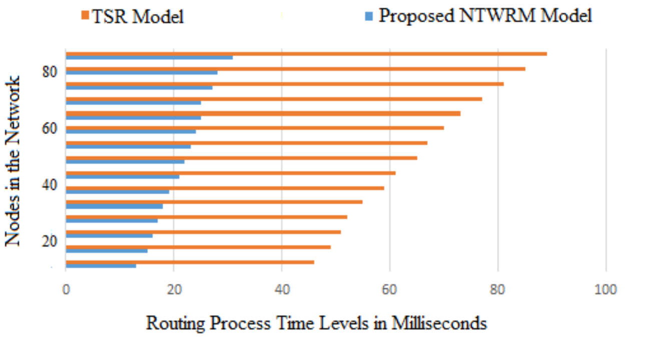


Figure 5. Routing process time levels

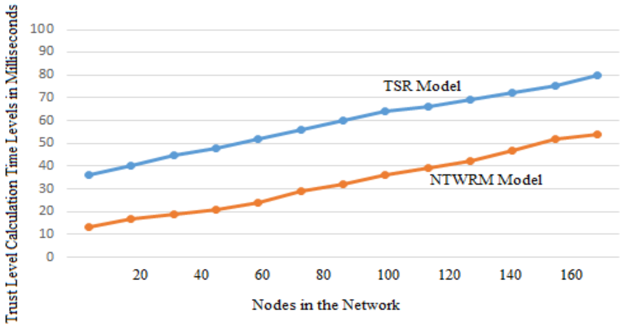


Figure 6. Trust level calculation time levels

The absence of prior knowledge on the other co-operating nodes results in the sharing of resources between trusted and untrusted nodes. There is also the need to formalize trustworthiness so that only the trusted nodes can share resources. MANET's dynamic and volatile nature makes many attacks vulnerable, leading to less security. The development of a safe MANET environment is an essential feature of MANET. The Figure 6 clearly indicates the trust level calculation time levels of the proposed and existing models. The trust levels of the proposed model are high when compared to traditional methods.

In recent years several MANET routing strategies have been designed, given the importance of routing protocols in complex multihop networks. The key characteristic of the proposed protocols for routing the packets can be guided from its present location, without using any mechanism for route discovery because routes are saved, if the node knows where a particular destination is. The route security levels of the proposed and traditional models are indicated in Figure 7. The route security levels of the proposed model are high when compared to traditional methods.

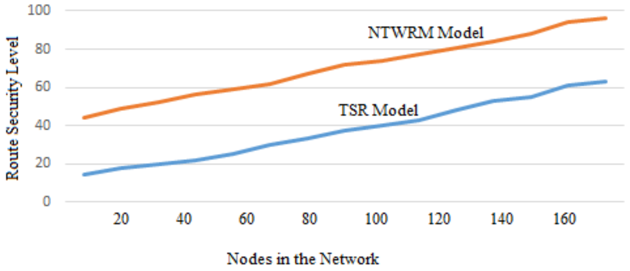


Figure 7. Route security level

The proposed model uses keys for verification of the authentication of the nodes for calculating trust factors. The proposed model generates the keys that are used one time and the key generation time levels of the proposed and traditional models are included in Figure 8.

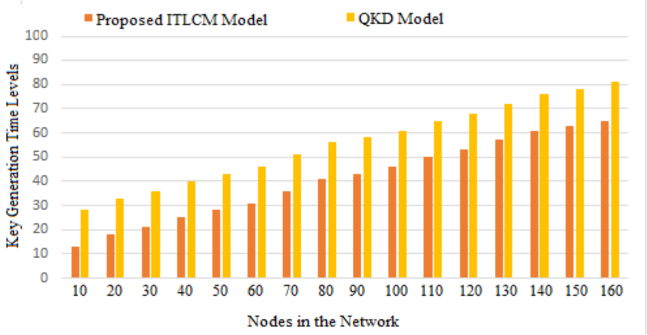


Figure 8. Key generation time levels

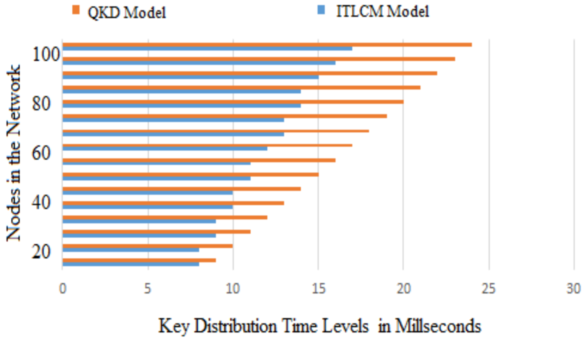


Figure 9. Key distribution time levels

The keys generated need to be distributed among the trusted nodes for performing trust calculation and updating. The proposed model is compared with the traditional models and the key distribution time levels are indicated in Figure 9.

The packet delivery rate indicates the count of packets that are successfully transmitted from sender to receiver. The packet delivery rate of the proposed and traditional methods is clearly depicted in Figure 10. The packet delivery rate of the proposed model is high when compared to the existing model. The packet delivery rate of the proposed model and traditional models are illustrated in Table 2.

Table 2. Packet delivery ratio (%)

Nodes Considered	QKD Model	ITLCM Model
20	29	49
40	35	55
60	40	70
80	43	73
100	50	75
120	50	80
140	58	84
160	60	94

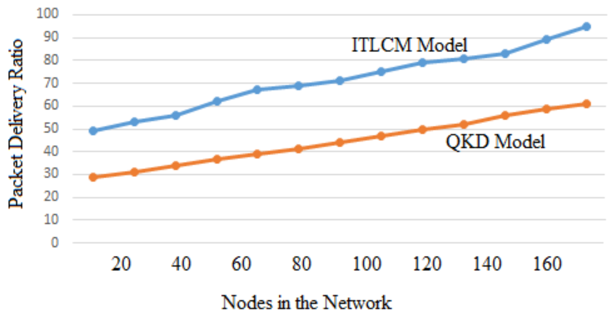


Figure 10. Packet delivery ratio

The packet loss rate indicates the count of packets that are dropped during data transmission from sender to receiver. The packet loss rate of the proposed and traditional methods is clearly depicted in Figure 11. The packet loss rate of the proposed model is less when compared to the existing model. The packet loss rate of the proposed model and traditional models are illustrated in Table 3.

Table 3. Packet loss ratio (%)

Nodes Considered	QKD Model	ITLCM Model
100	20	55
120	22	60
140	23	62
160	24	65
180	25	70
200	26	73
220	28	76
240	29	78

The mean end-to-end delay between both the origin and destination nodes is the mean value of the end-to-end delay. End-to-end delay is the cumulative time it takes to send the packet to its destination from source. This involves the delay in the data packets transmission due to the process of route discovery and the traffic. The End to End Delay levels are depicted in Figure 12. The end-to-end delay of a MANET is a crucial performance metric for real-time or capable of connecting. It is the overall amount of time it takes for a single packet to transit from its source node to its destination node in a MANET. The End to End delay levels are indicated in Table 4.

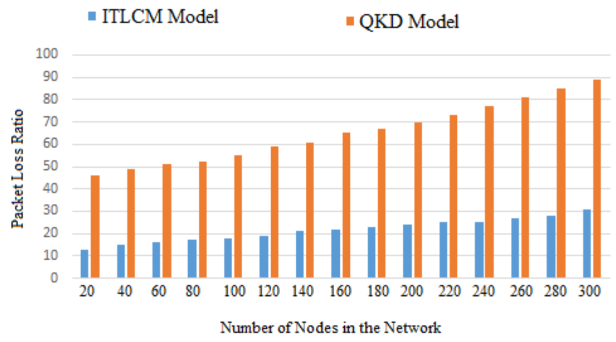


Figure 11. Packet loss ratio

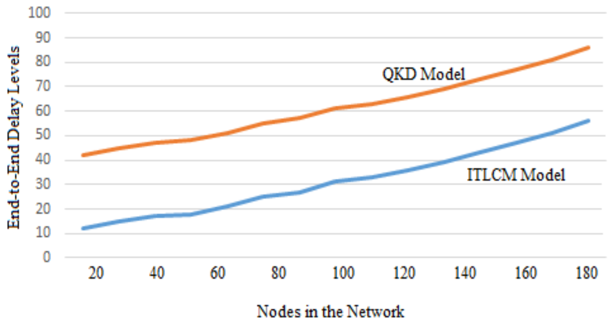


Figure 12. End to end delay

Table 4. End-to-end delay

Nodes Considered	QKD Model	ITLCM Model
20	12	42
40	18	45
60	20	50
80	25	55
100	30	60
120	35	65
140	40	70
160	50	80
180	60	86

5. CONCLUSIONS

The MANET is an ad hoc network with multiple hops and a self-disciplinary system which does not rely on fixed contact. The Ad Hoc network consists of a collection of structural nodes that switch around and changes dynamically. The nodes connect to others through the wireless network where each network node has the double functions of an endpoint or a router. Due to their future uses, mobile ad-hoc network has drawn significant interest in the research community. The inherent features of those networks, however, make them vulnerable to a wide range of attacks. In ad hoc networks, trust management is crucial as any node may join and any node leaves at any time. For this reason, the ad hoc network is too vulnerable to attacks of many types. The consistency of the network's service therefore becomes an essential problem for packet droppings. The proposed model calculates a trust value for each node and increases this value based on if the packet can be forwarded and whether the request is forwarded. In the proposed work, a Neighbor Trust Weight based Routing Model is implemented that provides a secure route and then for key management system, a Trust Level based Cryptography Model is introduced for secure key distribution that improves the security levels of the network that improves system performance. In the proposed model, a trusted node is selected to monitor all of the nodes in the routing process to create a stable multi-key distribution environment that enhances MANET performance. In future automatic adjusting of trust values and automatic updating of routing process can be performed that still improves the network performance.

REFERENCES

[1] Xia, H., Jia, Z., Li, X., Ju, L., Sha, E.H.M. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Networks, 11(7): 2096-2114. https://doi.org/10.1016/j.adhoc.2012.02.009

[2] Gharehkoolchian, M., Hemmatyar, A.M., Izadi, M. (2015). Improving security issues in MANET AODV routing protocol. In International Conference on Ad Hoc Networks, pp. 237-250. https://doi.org/10.1007/978-3-319-25067-0_19

[3] Airehrour, D., Gutierrez, J., Ray, S.K. (2015). GradeTrust: A secure trust based routing protocol for MANETs. In 2015 International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, Australia, pp. 65-70. https://doi.org/10.1109/ATNAC.2015.7366790

[4] Patel, V.H., Zaveri, M.A., Rath, H.K. (2015). Trust based routing in mobile ad-hoc networks. Lecture Notes on Software Engineering, 3(4): 318.

[5] Gupta, P., Goel, P., Varshney, P., Tyagi, N. (2019). Reliability factor based AODV protocol: Prevention of black hole attack in MANET. In Smart Innovations in Communication and Computational Sciences, pp. 271-279. https://doi.org/10.1007/978-981-13-2414-7_26

[6] Mahdi, M.A., Wan, T.C., Abdullah, R. (2019). Performance evaluation of MANETs routing protocols in non-uniform node density topology. In 10th International Conference on Robotics, Vision, Signal Processing and Power Applications, pp. 411-418. https://doi.org/10.1007/978-981-13-6447-1_52

[7] Mandhare, A., Kadam, S. (2019). Performance analysis of trust-based routing protocol for MANET. In Computing, Communication and Signal Processing, pp. 389-397. https://doi.org/10.1007/978-981-13-1513-8_41

[8] Medadian, M., Yektaie, M.H., Rahmani, A.M. (2009). Combat with Black hole attack in AODV routing protocol in MANET. In 2009 First Asian Himalayas International Conference on Internet, Kathmundu, Nepal, pp. 1-5. https://doi.org/10.1109/AHICI.2009.5340351

[9] Saudi, N.A.M., Arshad, M.A., Buja, A.G., Fadzil, A.F.A., Saidi, R.M. (2019). Mobile ad-hoc network (MANET) routing protocols: A performance assessment. In Proceedings of the third international conference on computing, mathematics and statistics (iCMS2017), pp. 53-59. https://doi.org/10.1007/978-981-13-7279-7_7

[10] Hemalatha, S., Mahesh, P.S. (2018). Energy optimization in directional advanced intruder handling AODV protocol in MANET. Swansea Printing Technology Ltd, 14: 935-960.

[11] Mohammadani, K., Khan, R.A., Memon, K.A., Hussaini, N.N., Awan, J.H., Kuar, R. (2018). Stress-based performance analysis of AODV & DSDV routing protocols in MANET. Engineering Science and Technology International Research Journal, 2(2): 1-6.

[12] Moudni, H., Er-rouidi, M., Mouncif, H., El Hadadi, B. (2016). Performance analysis of AODV routing protocol in MANET under the influence of routing attacks. In 2016 International Conference on Electrical and Information Technologies (ICEIT), Tangiers, Morocco, pp. 536-542. https://doi.org/10.1109/EITech.2016.7519658

[13] Rao, R.L., Satyanarayana, B., Kondaiah, B. (2018). Performance of CBIDS on AODV routing protocol against black hole attacks in MANET. International Journal of Scientific Research in Computer Science, Engineering and Information Technology.

[14] Singh, T., Singh, J., Sharma, S. (2017). Energy efficient secured routing protocol for MANETs. Wireless Networks, 23(4): 1001-1009. https://doi.org/10.1007/s11276-015-1176-9

[15] Jain, A.K., Tokekar, V. (2015). Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks. In 2015 International Conference on Pervasive Computing (ICPC), Pune, India, pp. 1-6. https://doi.org/10.1109/PERVASIVE.2015.7087174

[16] Singh, S., Mishra, A., Singh, U. (2016). Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm. In 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, pp. 1-6. https://doi.org/10.1109/CDAN.2016.7570906

[17] Tseng, F.H., Chiang, H.P., Chao, H.C. (2018). Black hole along with other attacks in MANETs: a survey. Journal of Information Processing Systems, 14(1): 56-78. https://doi.org/10.3745/JIPS.03.0090

[18] Sen, B., Meitei, M.G., Sharma, K., Ghose, M.K., Sinha, S. (2018). A trust-based intrusion detection system for mitigating blackhole attacks in MANET. In Advanced Computational and Communication Paradigms, pp. 765-775. https://doi.org/10.1007/978-981-10-8237-5_74

[19] Tan, S., Li, X., Dong, Q. (2015). Trust based routing mechanism for securing OSLR-based MANET. Ad Hoc Networks, 30: 84-98. https://doi.org/10.1016/j.adhoc.2015.03.004

[20] Ahmed, F., Rashid, S., Rahman, M. (2016). Impact of Black-hole and Jellyfish Attacks in MANET using HTTP Traffic. Doctoral dissertation, BRAC University.

[21] Ali, A.K., Sharma, B., Sharma, U.M. (2016). Impact analysis of JellyFish attack in MANETs. ADBU Journal of Engineering Technology, 4.

[22] Del-Valle-Soto, C., Mex-Perera, C., Monroy, R., Nolazco-Flores, J.A. (2015). On the routing protocol influence on the resilience of wireless sensor networks to jamming attacks. Sensors, 15(4): 7619-7649. https://doi.org/10.3390/s150407619

[23] Pang, L., Wei, M., Li, H. (2019). Efficient and anonymous certificateless multi-message and multi-receiver signcryption scheme based on ECC. IEEE Access, 7: 24511-24526. https://doi.org/10.1109/ACCESS.2019.2900072

[24] Guan, Z., Zhang, Y., Wu, L., Wu, J., Li, J., Ma, Y., Hu, J. (2019). APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. Journal of Network and Computer Applications, 125: 82-92.

https://doi.org/10.1016/j.jnca.2018.09.019

[25] Gao, R., Zeng, J., Deng, L. (2018). Efficient certificateless anonymous multi-receiver encryption scheme without bilinear parings. Mathematical Problems in Engineering, 2018: 1486437. https://doi.org/10.1155/2018/1486437

[26] Rajesh, R., Ramakrishnan, M., Sugumar, B. (2017). A modest approach on MANET using certificateless cryptography. In 2017 International Conference on Intelligent Sustainable Systems (ICISS), pp. 1197-1204. https://doi.org/10.1109/ISS1.2017.8389376

[27] Sugumar, B., Ramakrishnan, M. (2018). An exhaustive investigation of security issues tended to by different cryptographic algorithms.

[28] Sayid, J., Sayid, I., Kar, J. (2016). Certificateless public key cryptography: A research survey. International Journal of Security and Its Applications, 10(7): 103-118. http://dx.doi.org/10.14257/ijsia.2016.10.7.10