A Trusted Data Transmission Protocol for Mobile Ad-Hoc Networks

Shaik Noor Mohammad

Abstract*: *Nowadays, data transmission happens in all the system architecture to deliver vital information from one device to another device. Thus, this process has become an important requirement factor in the communication procedure in mobile ad-hoc network. But there are crucial security challenges, which should be addressed for effective communication. In this paper, we propose a secure and effective data transmission scheme to share vital information between mobile nodes. This protocol is protected against various security attacks. In addition to this, the results are discussed of the proposed method to check the effectiveness in the implementation cost, communication cost, and power consumption.

Keywords: Attack; Communication; Computational; Data; MANET; Security.

I. INTRODUCTION

A mobile ad-hoc network is a collection of independent movable nodes that can communicate with each other via radio waves. Mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets [1, 2]. The data transmission process is shown in Fig. 1.

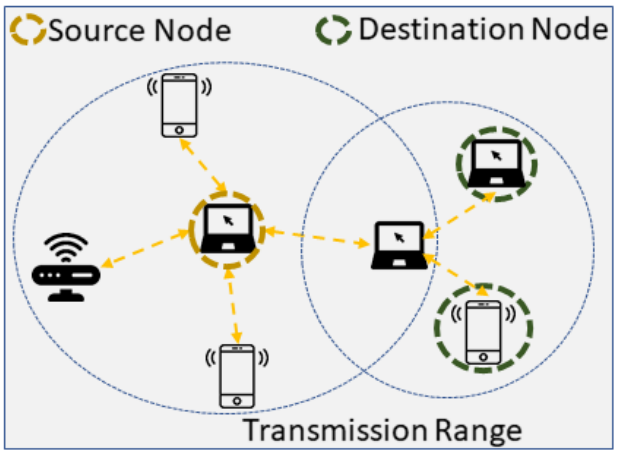

Fig. 1 Communication Between Different Mobile Nodes

The MANET structure has various types based on their applications [3, 4] and these applications are road safety, sensors for body/environment, vehicular communication, home, peer-to-peer messaging, health, disaster rescue operations, robots, air/land/navy defense, etc.

Revised Manuscript Received on June 05, 2019

Shaik Noor Mohammad, Research Scholar, Department of Electronics & Communication Engineering, Sri Satya Sai University of Technology and Medical Sciences. Sehore, Bhopal (M.P) India.

The MANET has following different characteristics as distributed processing, multi-hop routing, autonomous terminal, dynamic topology, light-weight terminal, shared physical medium. In general, data is transferred over a public channel and thus, there are different ways to intercept this data. Therefore, there is a requirement of secure communication method, which can deliver meaningful information to the receiver securely. Next, if data is not available to the receiver end within the fixed amount of time, then it might be useless for the receiver and thus, the data transmission scheme should also perform all required operations quickly before sending packets to the receiver(s). Hence, the communication system should be designed using lightweight operations to utilize minimum computational resources.

A. Related Works

There are various mobile data transmission schemes to exchange meaningful information from one node to another node. We discuss on various features and issues of some recent mobile data transmission mechanisms. In 2015, Yan et al. [7] proposed a batch-signature verification system to preserve privacy of mobile users, and in this mechanism, they have used the concept of bi-linear. But this scheme [7] needs high cost operations during the implementation and thus, it is not suitable in MANETs. Alomari [8] came up with an enhanced mutual authentication method using symmetric key cryptography for mobile nodes to exchange messages and therefore, there is a major issue of key sharing in MANETs for both (new and existing) nodes. Moreover, the secure storage of the secret key is also an important issue in MANETs because an intruder may attempt to steal credentials from a storage memory of these nodes. Shanthi and Murugan [9] suggested a group key agreement mechanism based on bi-linear Diffie-Hellman concept to transfer messages securely between mobile nodes. In this method [9], nodes firstly generate a pair-wise for a hop-by-hop group key agreement method to check the exactness of a transient key. But the performance of this mechanism is not appropriate in MANETs because of high cost operations.

In 2018, Malhotra et al. [10] proposed an authentication protocol using symmetric key concept for secure data transmission in the mobile ad-hoc networks, but this protocol has security issues of different attacks (i.e., modification**,** impersonation, replay, man-in-the-middle, and sybil). Moreover, the scheme [10] requires very high amount of computational resources due to usage of high-cost operations (i.e., random number generation). Therefore, the power consumption is also extremely high in [10]. Brindha et al. [11] came up with an authentication mechanism to improve

security concerns in MANETs, but this method is susceptible to replay, man-in-the-middle, and sybil attacks. Further, this protocol [11] is weak in the performance due to usage of high computational operations, and this leads to very high-power consumption. Thiyagarajan et al. [12] proposed an authentication protocol to improve security of the system using RSA public key cryptosystem. However, the mechanism [12] is vulnerable to replay and man-in-the-middle attacks. Moreover, the communication overhead is very high in [12] and thus, this is not suitable for data transmission in MANETs.

From the literature survey, we understand that there are various data transmission mechanisms for MANETs, but still there are different security and performance problems. To overcome these issues, we come up with an advanced and trusted communication mechanism for MANETs.

The paper is organized in the following manner. Section II presents the network model and discussion on possible security issues in MANETs. In Section III, we propose an efficient and secure communication protocol for mobile ad-hoc network to exchange useful information. Section IV presents performance results of the proposed method and these results are compared with other relevant data transmission systems. After that, we do security analysis on the suggested protocol to check its security strengths in Section V. Finally, conclude this paper in Section VI.

II. NETWORK MODEL AND PROBLEM STATEMENT

The MANET structure includes different types of mobile nodes, e.g., computer machine, mobile phone, wireless sensor, etc. and they transmit vital information from one end to another side via a public channel. Fig. 2 shows the network model in which different mobile nodes are shown for the registration and communication processes.

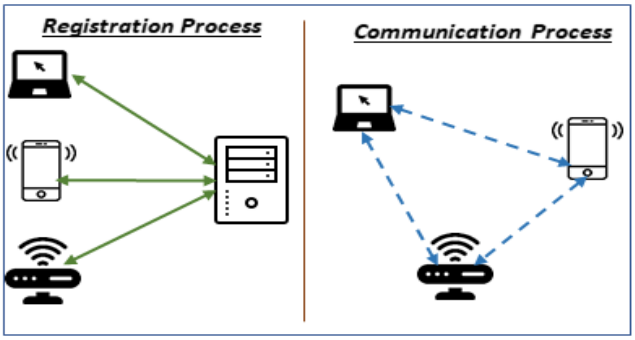

Fig. 2 The Network Model for Mobile Communication

Initially, mobile nodes should register with the server to become a legitimate mobile user of the system. After that, they can communicate with other registered mobile nodes after verifying each other mutually. These mobile nodes have a smart card or chip to store some important values and this card/chip is fixed into a mobile node during the registration phase.

When two mobile nodes exchange messages with each other over a common channel, an adversary may attempt to disturb this communication by doing malicious activities, i.e., modification in messages, stop/delay in packet transmission, impersonation for a legitimate user, understand private messages, etc. [5, 6]. The description on each security concern is as follows:

1. ***Modification Attack*:** An insider user attempts to modify packets to disrupt the network. For example, in the modification attack, an intruder tries to attract all traffic from a particular area through a compromised node. It is especially effective in routing protocols that use advertised information such as remaining energy, data transmission traffic, nearest node to the destination in the route discovery process.
2. **Dropping Attack:** Malicious or selfish nodes deliberately drop all packets that are not destined for them. While malicious nodes attempt to disrupt the network connection, selfish nodes try to preserve their resources. Dropping attacks can prevent end-to-end communications between nodes if the dropping node is at a critical point. It might also reduce the network performance by causing data packets to be retransmitted, new routes to the destination to be discovered.
3. **Man-in-the-middle Attack:** This attack is difficult to identify and defend against an adversary's malicious actions. Moreover, a man-in-the-middle (MITM) attack generally is not dependent on the process of infecting computers at the system. Though, it depends on the communication equipment between two systems. For an example, an adversary offers free Wi-Fi at a public location and in this way, s/he may perform a man-in-the-middle attack.
4. **Impersonation Attack:** An adversary takes the identity of a legal user (say *A*) of the communication system. Then, an attacker computes various parameter to send a forged login/message request to another valid user (Say *B*) behalf of a user-*A*. If this request is accepted by user-*B*, then an adversary is successful in performing an impersonation attack. Here, user-*A* does not have any knowledge of this communication. Generally, an attacker succeeds in this malicious activity if and only if s/he has all required values to compute a fake login/message request.

III. THE PROPOSED MOBILE COMMUNICATION PROTOCOL

We suggest a new authentication scheme to transmit data between mobile nodes. The proposed protocol mainly includes three phases as (1) registration (2) login and (3) authentication. These phases are described in detail as follows.

A. Registration Phase

This process is one-time task of users and it is essential for non-registered mobile node users because they cannot communicate with each other without being a legitimate user of the system. To register with the server, a mobile user (MU_i) and the server (S) do the following:

1. MU_i chooses his/her identity (ID_{MU_i}), passcode (PC_{MU_i}), and one random number as x_i. Then, MU_i

computes $A_i = h(ID_{MU_i} \oplus PC_{MU_i} || x_i \oplus ID_{MU_i})$ and sends $\{ ID_{MU_i}, A_i \}$ to the server (S) securely.

2. S computes $B_i = h(ID_{MU_i} \oplus A_i || y \oplus ID_{MU_i})$, $C_i = B_i \oplus h(A_i || ID_{MU_i})$, $D_i = A_i \oplus B_i$, $E_i = h(A_i || B_i) \oplus h(\mathcal{T} || MK_S || ID_{MU_i})$. Here, MK_S is the 256-bit server's secret key and $\mathcal{T}$ is the generation time-stamp of MK_S. Then, S saves C_i, D_i, E_i in a memory of a mobile node (MN_i). Furthermore, S stores $\{List_{ID_{MU_i}}, List_{E_i}\}$ into MN_i's memory.
3. MU_i calculates $F_i = h(ID_{MU_i} \oplus PC_{MU_i}) \oplus x_i$ and stores D_i into MN_i's memory.

B. Login Phase

To transmit data with another mobile node (MU_j), MU_i should prove his/her legitimacy and for this, s/he should enter his/her private credentials to send a login request to MU_j. The procedure is as follows for the proposed login phase:

1. MU_i inserts ID_{MU_i}, PC_{MU_i} and calculates $x = F_i \oplus h(ID_{MU_i} \oplus PC_{MU_i})$, $A_i = h(ID_{MU_i} \oplus PC_{MU_i} || x \oplus ID_{MU_i})$, $B_i = C_i \oplus h(A_i || ID_{MU_i})$, $D'_i = A_i \oplus B_i$. If D'_i and D_i are equal, then only the system proceeds to the next step. Otherwise the session is terminated immediately.
2. MU_i does $X_i = h(E_i \oplus E_j \oplus T_1)$ and sends a login request as $\{ID_{MU_i}, X_i, T_1\}$ to MU_j.

C. Authentication Phase

To verify the received request, MU_j performs as follows and if it is valid, then MU_j creates a connection to exchange important information through a public channel.

1. MU_j inserts ID_{MU_j}, PC_{MU_j} and calculates $x_j = F_j \oplus h(ID_{MU_j} \oplus PC_{MU_j})$, $A_j = h(ID_{MU_j} \oplus PC_{MU_j} || x_j \oplus ID_{MU_j})$, $B_j = C_j \oplus h(A_j || ID_{MU_j})$, $D'_j = A_j \oplus B_j$. If D'_j and D_j are the same value, then only the system proceeds to the next step. In other cases, the session is ended directly.
2. MU_j checks the freshness of an obtained request by doing $\Delta T \leq T_1 - T_2$. If it is valid, then MU_j computes $X'_i = h(E_i \oplus E_j \oplus T_1)$. If $X'_i \neq X_i$, then the session is stopped instantly. If X'_i and X_i are equal, then only the system understands that $\{ID_{MU_i}, X_i, T_1\}$ is sent by MU_i. Further, MU_j and MU_i computes the common session key as $SK = h(ID_{MU_j} || E_j || X_i)$, and this key is valid for a limited period only. If the session key is expired, then both (MU_i and MU_j) should perform the login and authentication phases again.

IV. PERFORMANCE ANALYSIS ON THE PROPOSED SCHEME

We consider the Raspberry Pi 3B platform for the implementation, which has Quad Core 1.2GHz Broadcom BCM2837 CPU, 1 GB RAM, and 2.5 A power. Different cryptographic operations are implemented on this embedded device platform and the execution time of each operation is 0.1074 milliseconds (*ms*) for one-way hash SHA 256-bit ($T_{h(\cdot)}$), 300259.4031 *ms* for random nonce (T_{RN}), 11.6482 *ms* for elliptic curve (T_{EC}), 2.3472 *ms* for advanced encryption standard (T_{AES}), 6.0943 *ms* for RSA encryption (T_{ERSA}), and 215.6940 *ms* for RSA decryption (T_{DRSA}). Table I shows the total number of required cryptographic operations to establish a connection for data transmission ([10], [11], [12], and the proposed protocol) between mobile nodes. By considering the execution time of each cryptographic operation, the total implementation time is calculated for different communication schemes and the comparison of the execution time is shown in Fig. 3. Data transmission methods ([10] and [11]) take very high time in the implementation because they have used a good number of elliptic curve, random nonce generation, and AES operations. From this comparison, the proposed method needs extremely less time for the execution and thus, it is very quick for data transmission.

Table I Computational Cost Evaluation for Different Communication Methods

Schemes	Operations
Malhotra et al. [10]	$2\ T_{RN} + 4\ T_{h(\cdot)}$
Brindha et al. [11]	$1\ T_{RN} + 7\ T_{EC} + 3\ T_{h(\cdot)} + 2\ T_{AES}$
Thiyagarajan et al. [12]	$1\ T_{ERSA} + 1\ T_{DRSA}$
Proposed	$10\ T_{h(\cdot)}$

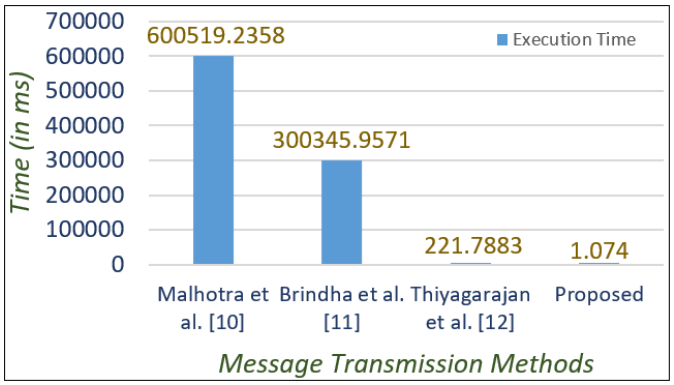

Fig. 3 Execution Time for Various Communication Schemes

Next, the data transmission scheme sends different values to another mobile node and thus, it needs a fixed amount of memory to establish a connection with this node. This cost is known as the communication cost. We assume that an identity takes 10 bytes; an RSA needs 384 bytes; a time-stamp requires 8 bytes; an elliptic curve takes 64 bytes; and a one-way hash needs 32 bytes (for SHA-2). By considering this memory cost for different parameters, we calculate the communication cost for the proposed scheme, [10], [11], and [12]. The suggested method requires 1 (one-way hash), 1 (time-stamp), and 1 (identity). The protocol [10] takes 2 (one-way hash) and 2 (identity). In the scheme [11], 2 (elliptic curve) and 1 (one-way hash) are required for the communication cost. The communication system [12] needs 1 (RSA) parameter. Further, the graphical representation is prepared

for the requirement of number of bytes in various communication protocols and it is shown in Fig. 4.

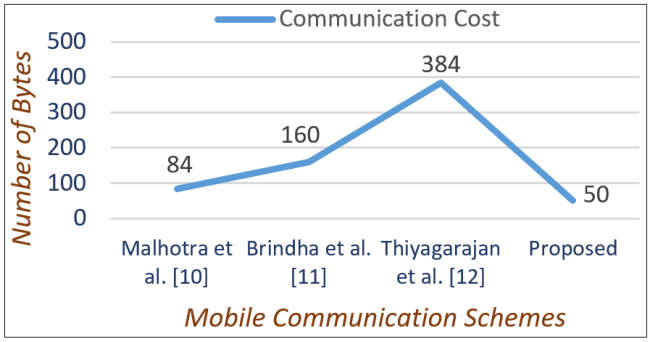

Fig. 4 Communication Cost Comparison among Various Mobile Data Transmission Protocols

The power consumption is computed using the formula $PC = P_{CPU} * ET$, where $PC =$ power consumption, $P_{CPU} =$ maximum CPU power (12.5 W), and $ET =$ execution time. Therefore, we have calculated the power consumption for the proposed method, [10], [11], and [12]. In this calculation, we consider the execution time from Fig. 3 and the comparison on the power consumption is displayed in Fig. 5.

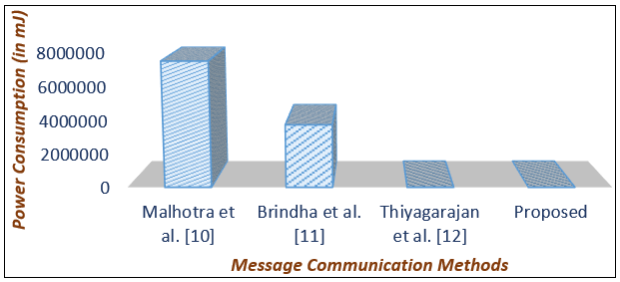

Fig. 4 Power Consumption Requirement in Different Data Transmission Schemes

V. SECURITY ANALYSIS ON THE PROPOSED PROTOCOL

We do security analysis of the suggested data transmission scheme to check its security strengths and for this, we have described how different security attacks are not feasible in the proposed method. The description on each attack is as follows.

A. Modification Attack

Packets are transferred via a public channel, and an adversary ($\mathcal{A}$) normally captures these packets during the data transmission phase. After that, s/he tries to change some information in a message and then, s/he sends it to mobile node. If the receiver accepts this updated message, then $\mathcal{A}$ is screenful to perform a modification attack. According to the proposed protocol, MU_i and MU_j use the session key (SK) to communicate with each other and this key is fresh for each new session. Therefore, $\mathcal{A}$ should know SK, which is computed as $h(ID_{MU_j}||E_j||X_i)$ and for this, $\mathcal{A}$ should have knowledge of ID_{MU_j}, E_j, T_1, and X_i. Here, $\mathcal{A}$ might know X_i and T_1 from a common channel, but it is hard to get ID_{MU_j} and E_j because these values are not available publicly. Further, if $\mathcal{A}$ manages to get all required values through searching (it is only possible if $\mathcal{A}$ is a registered with the server.), then the session key is expired and there is no use of these parameters. Ultimately, $\mathcal{A}$ is unable to do any changes in communication between MU_i and MU_j. Hence, a modification attack is feasible in the proposed protocol.

B. Sybil Attack

An adversary uses different users' identity to generate login requests and then, s/he sends these requests to the different mobile nodes. At this point, if the receiver accepts an obtained request, then a sybil attack is feasible in the system. According to the proposed scheme, $\mathcal{A}$ should know $ID_{MU_i}, E_i, E_j, ID_{MU_j}$ to compute X_i and after that, s/he can send a login request to a mobile node in order to transmit meaningful information. However, $\mathcal{A}$ does not know E_i and E_j. Thus, an adversary can proceed further to perform malicious activities. As a result, a sybil attack is not feasible in the suggested method.

C. Man-in-the-Middle Attack

In general, data is sent over an insecure communication channel and thus, $\mathcal{A}$ has an opportunity to get this data directly. If $\mathcal{A}$ can retrieve some meaningful information from this captured data, then a man-in-the-middle attack is possible. To understand transmitted messages, $\mathcal{A}$ requires the session key because MU_i and MU_j practice SK to exchange vital information with each other. We have already explained that $\mathcal{A}$ cannot compute SK due to unavailability of all required values. For this reason, an adversary is not able to perform a man-in-the-middle attack in the suggested method.

D. Replay Attack

If $\mathcal{A}$ is able to delay/stop transmitted login request/message; s/he sends this request/message later to a mobile node, and the receiver accepts the delayed login/message, then the protocol is vulnerable to a replay attack. As per the proposed scheme, U_i sends a login request as $\{ID_{MU_i}, X_i, T_1\}$ to MU_j through a common channel. Here, an attacker ($\mathcal{A}$) may want to delay this request. To do this, $\mathcal{A}$ need to compute X_i because T_1 is used in the computation of X_i and the receiver checks the freshness of $\{ID_{MU_i}, X_i, T_1\}$through ΔT before proceeding to the next step. X_i is calculated as $h(E_i \oplus E_j \oplus T_1)$ in the proposed scheme and $\mathcal{A}$ is not able to compute again X_i. Therefore, $\mathcal{A}$ does not have any opportunity to carry out a replay attack in the suggested method.

E. Impersonation Attack

If an adversary is able to impersonate any legal mobile user by sending forged login credentials, then an impersonation attack is achievable in the data transmission system. To do this, $\mathcal{A}$ should compute X_i ($=h(E_i \oplus E_j \oplus T_1)$). But an adversary does not have knowledge of E_j and E_i. Further, E_i is calculated as $h(A_i||B_i) \oplus h(\mathcal{T}||MK_S||ID_{MU_i})$ and $\mathcal{A}$ does not have MK_S, A_i, B_i, and $\mathcal{T}$. As a result, $\mathcal{A}$ is not able to proceed to carry out any illegal activity to impersonate mobile nodes. Hence, an impersonation attack is not feasible in the suggested protocol.

Next, we have compared the proposed scheme with

other relevant communication methods ([10], [11], and [12]) in terms of security and it is shown in Table II. **S1**: *Modification*; **S2**: *Impersonation*; **S3**: *Replay*; **S4**: *Man-in-the-middle*; **S5**: *Sybil*; √: *Secure*; ∅:*Vulnerable;*

Table II Security Attacks Comparison for Various Data Transmission Schemes

Schemes	S1	S2	S3	S4	S5
Malhotra et al. [10]	∅	∅	∅	∅	∅
Brindha et al. [11]	√	√	∅	∅	∅
Thiyagarajan et al. [12]	∅	√	∅	∅	√
Proposed	√	√	√	√	√

VI. CONCLUSION

We discuss the importance of data transmission between mobile nodes in the fast-growing world. Then, we describe various security concerns in the mobile ad hoc network architecture and after that, we have proposed an efficient and secure data transmission protocol. The results show that the suggested method can withstand against various security attacks, i.e., modification, sybil, man-in-the-middle, replay, and impersonation. Further, the proposed scheme takes very low time in the implementation and it requires very less amount memory during the communication. Therefore, the proposed scheme consumes less power during the implementation. For all these reasons, the suggested protocol can be practiced in different smart city applications to exchange important data securely and efficiently.

REFERENCES

1. Junhai, L., Danxia, Y., Liu, X., & Mingyu, F. (2009). A survey of multicast routing protocols for mobile ad-hoc networks. IEEE communications surveys & tutorials, 11(1), 78-91.
2. Tarique, M., Tepe, K. E., Adibi, S., & Erfani, S. (2009). Survey of multipath routing protocols for mobile ad hoc networks. Journal of network and computer applications, 32(6), 1125-1143.
3. Kiess, W., & Mauve, M. (2007). A survey on real-world implementations of mobile ad-hoc networks. Ad Hoc Networks, 5(3), 324-339.
4. Ray, P. P. (2018). A survey on Internet of Things architectures. Journal of King Saud University-Computer and Information Sciences, 30(3), 291-319.
5. Cho, J. H., Swami, A., & Chen, R. (2011). A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 13(4), 562-583.
6. Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. IEEE communications surveys & tutorials, 15(4), 2027-2045.
7. Yan, Z., Feng, W., & Wang, P. (2015). Anonymous authentication for trustworthy pervasive social networking. IEEE Transactions on Computational Social Systems, 2(3), 88-98.
8. Alomari, A. (2015). Mutual authentication and updating the authentication key in manets. Wireless Personal Communications, 81(3), 1031- 1043.
9. Shanthi, K., & Murugan, D. (2017). Pair-wise key agreement and hop-by-hop authentication protocol for MANET. Wireless Networks, 23(4), 1025-1033.
10. Malhotra, S., & Trivedi, M. C. (2018). Symmetric Key Based Authentication Mechanism for Secure Communication in MANETs. In Intelligent Communication and Computational Technologies (pp. 171-180). Springer, Singapore.
11. Brindha, V., Karthikeyan, T., & Manimegalai, P. (2018). Fuzzy enhanced secure multicast routing for improving authentication in MANET. Cluster Computing, 1-9.
12. Thiyagarajan, R., & Priya, B. M. (2019). An enhancement of EAACK using P2P ACK and RSA public key cryptography. Measurement, 136, 116-121.

AUTHORS PROFILE

Shaik Noor Mohammad, Research Scholar, Department of Electronics & Communication Engineering, Sri Satya Sai University of Technology and Medical Sciences. Sehore, Bhopal (M.P) India.