A Secure Lightweight Distributed Authentication Framework for MANets

Alwi M Bamhdi†, Hushmat Amin Kar††

† Department of Computer Sciences, College of Computing (Al Qunfudhah), Umm Al-Qura University, Saudi Arabia
†† Department of Electronics & Communication, National Institute of Technology Srinagar, Kashmir, India

Summary
The demand for mobile ad-hoc networks is increased tremendously, almost in every application area. The wireless and infrastructure-less features of these networks have explored a plethora of application areas. Apart from the numerous benefits of using MANets, certain issues hinder the users from exploring its full potential. Security is one of the primary issues that need to be addressed. This paper presents a secure authentication framework for mobile ad-hoc networks. The framework uses hybrid encryption techniques and authenticates the nodes in a distributed manner. The framework takes into consideration the resource-constrained devices in mobile ad-hoc networks and uses lightweight encryption techniques to achieve a secure environment.

Key words:
MANet, Security, Adhoc Networks, Authentication.

1. Introduction

Ad-hoc networks have great potential in a variety of applications due to its self-configuration and self-maintenance properties [1]. These networks are flexible, infrastructure-less and distributed in nature. Most of the ad hoc networks use wireless communication technologies which makes the network mobile and flexible, known as mobile ad hoc networks (MANets). These mobile nodes also act as routers to make the network more efficient and robust. The mobile nature of the network leads to some challenges like dynamic routing, battery life, security etc. that need to be addressed. Among all the challenges, security is the key aspect that is essential to provide a secure network environment. The conventional security mechanism like centralized control is not applicable ad-hoc networks for providing security features like authentication, access control etc. because of its dynamic and agile nature. Due to these factors, the Adhoc network is susceptible to various kinds of attacks, which can be categorized as [2]:

(i) Active attacks

In this type of attack, a non-legitimate user either changes some data field or creates false information. Which is then transmitted to the target node to gain access to the network resource. The attacks like sinkholes, fabrication, denial of service (DoS), wormhole, modification and Sybil belong to this category.

(ii) Passive Attacks

This type of attack involves observation of information Being transmitted. Passive attacks do not modify system resources. These types of attacks are difficult to identify. The security attack like eavesdropping, traffic analysis and monitoring falls in this category. One of the distinguishing characteristics of MANet from the security architecture viewpoint is the absence of a clear line of defence. The wireless medium is available for both authorized users and attackers. There is no clearly defined area where it is possible to install traffic management or access control systems. The current routing protocols like DSDV, DSR and LBR etc. presume that nodes are operating in a trusted environment. Consequently, the attacker will exploit the loopholes of the network.

An efficient security mechanism is required, which will ensure the security goals, i.e. availability, integrity, confidentiality, authenticity, non-repudiation, authorization, and anonymity in ad hoc networks. The security mechanism should have full safety spanning the whole protocol stack to accomplish this objective. The security concerns in each layer are listed in Table 1 [3].

Table 1: Security Concerns of Each Layer

Layer	Security Issues
Application Layer	Identification and prevention of Malicious codes
Transport Layer	Ensuring end-to-end encryption and authentication.
Network Layer	Secure and efficient Routing.
Link Layer	Securing MAC protocols.
Physical Layer	Preventing Denial of service and Signal Jamming.

When the security features are embedded in the network, it will create an overhead, which in turn will affect the

Manuscript received November 5, 2020
Manuscript revised November 20, 2020
https://doi.org/10.22937/IJCSNS.2020.20.11.8

network performance [4]. As the security of ad hoc networks has become a prime factor, so there should be a trade-off between security measures and network performance. Authentication of nodes remains the primary security issue that needs to be addressed. There are two ways to authenticate a node in ad-hoc networks, i.e. direct and indirect [5-6]. Direct authentication involves the use of pre-shared keys while indirect authentication uses certificate authority for authenticating the nodes. The transmission of data is secured by encrypting the data at the source node and then transmitting it to the other node.

This paper presents a new authentication framework for Adhoc network. The proposed frameworks use hybrid encryption techniques to ensure authentication and data security. The rest of the paper is organized as; section II gives the related work; section III presents the proposed framework. In section IV simulation and results are discussed. Finally, section V concludes the work presented in the paper.

2. Related Work

Several researchers have proposed different mechanisms to create a secure environment for MANET nodes so that only authorized nodes can access the networks and securely communicate with each other. This section reviews various approaches proposed to make the MANET Environment Secure.

A study by [7], presented an enhanced secure routing multipath scheme. In this study, the authors first analysed various multipath algorithms. They then proposed an enhanced secure multipath routing scheme that helps the nodes in the ad-hoc network to find routes efficiently.

A study by [8], proposed an approach to counter wormhole attacks in ad-hoc networks using AODV, DSR, and OLRS. Further, the authors discuss various modes of wormhole attacks and their interruption to the network. A study by [9], have proposed a routing algorithm that is based on trust management. In this approach, a field in the request frame represented the trust factor, based on the trust factor routing information is distributed in the network. A study by [10], proposed a similar approach based on trust as presented by authors in [9]. The authors contributed a composite trust-based public key management (CTPKM), which embraces network performance and removes some security concerns.

A study by [11], proposed an approach that ensures secure communication is characterized by quantum features, including non-cloning and teleportation to deal with the vulnerability of potentially corrupted nodes. A Random EPR-pair allocation scheme is also proposed. A study presents by authors in [12] gives a comparison of various trust-based mechanisms used in MANETS [12]. The authors have also shown the effect on network performance due to a change in trust management.

Authors in [13] have proposed a secure architecture that ensures the authentication of sensor node through several WSN's. Authors have proposed virtual certificate authority (VCA) as a prime approach for authentication in ad hoc networks.

A study by [14], suggested a routing protocol for MANET Known as Physical layer security-based routing protocol (PLSR) and ad-hoc on-demand distance vector forms the basis for PLSR protocol. The Authors in [15], have analysed the distance-based localization issue in MANets which is carried out with the help of cheating beacons. The work presented shows that with a minimal time rate, the heuristic algorithms provide improved accuracy for localization. A study by [16], studied the performance of various routing protocols and their security issues. The authors have focused specifically on Black Hole attacks in MANet. The authors have also presented a mechanism for identification and avoidance of black hole attacks in MANets. Authors in [17], have studied various security attacks like DoS, GreyHole, BlackHole and Sybil on vehicular adhoc networks (VANet). In this study, authors have also proposed a novel routing scheme that will identify and mitigate security threats. Authors in [18] have analysed the performance of the gateway discovery system with and without security for different parameters. The author in [19] have discussed various security concerns raised due to the dynamic topologies of the MANets.

A study by authors [20] has proposed a secure framework for MANET using deniable authentication known as Identity-based deniable Authentication (IBDA) protocol. The framework uses Elliptical Curve Cryptography (ECC) and an Identity-based cryptography system (IBC). Authors in study [21], have proposed an authentication mechanism for MANet using dynamic MANet on-demand (DYMO) protocol based on reinforced learning. The framework eliminates the use of third-party used for key distribution in MANets. A study by [22] proposed an efficient and secure routing protocol for MANets using Ant colony optimization (ACO) known as QOS Mobility-aware ACO (QMAA). Also, the authors in this study proposed a security algorithm called Secure-QMAA. The proposed framework guarantees efficient QoS performance and a secure environment. A study by [23], have proposed an authentication protocol based on certificate exchange. The framework makes use of the hash function for maintaining the authenticity of certificates.

A study by [24], proposed an efficient mechanism for securing the AODV routing protocol [24]. In this framework, the authors have shown that how before establishing the path nodes are authenticated using a digital certificate in HELLO packets. These path nodes allow mitigating several attacks on the AODV routing protocol. A study by [25], proposed the use of a secure Hash algorithm (SHA3–256) for securing the hybrid routing protocols in MANets. This framework achieves data integrity and authentication using hashed messages authentication code (HMAC). A study by [26], have proposed a method for securing the AODV routing protocol against blackhole attacks. The mechanism involves the authentication of each node during the route discovery phase to prevent black hole attack.

3. Proposed Framework

A secure framework for authentication of ad-hoc nodes is presented in this section. Several researchers have proposed mechanisms for authenticating nodes using an authentication server, but in most of the scenarios, adhoc network nodes do not have the communication capability for communicating with the server. The main aim of the framework is that the nodes in the MANet should be able to authenticate each other without using the central authority or Authentication server. Also, there is a mechanism for the transfer of information in a secure manner.

In this framework, every node before joining a network will be embedded with a group unique ID (GUID) and a hash function (PHOTON-128). The proposed system poses the way for authentication of both new nodes and old nodes. Figure 1 shows the framework of the proposed system.

1) Scenario 1: For new nodes

Consider a scenario, when a new node X wants to join the MANET network, it will send a probe request and its public P_X as shown in Figure 2. The other node Y Connected to the network will receive the packet and reply with a frame containing its public key P_Y and enquiry (a) regarding the identity of the node. Which is represented by one bit in the frame, viz 0→ old nodes and 1→ new nodes. Node X will generate a hash of GUID and will encrypt the hash GUID with P_Y and Option (either 0 or 1). Node Y, on the other hand, will decrypt the message and extract the hash of GUID using its private key K_Y. It then separately calculates the hash of its GUID and compares it with the received hash (GUID). If they match, it will transmit a frame containing GUID, symmetrical key and re-joining factor, encrypted with P_X to X. GUID is transmitted again to validate the existing Node Y in the network. The symmetric key is used for secure transmission and rejoining factor (RF) is used in case; the node gets disconnected from the network and wants to reconnect.

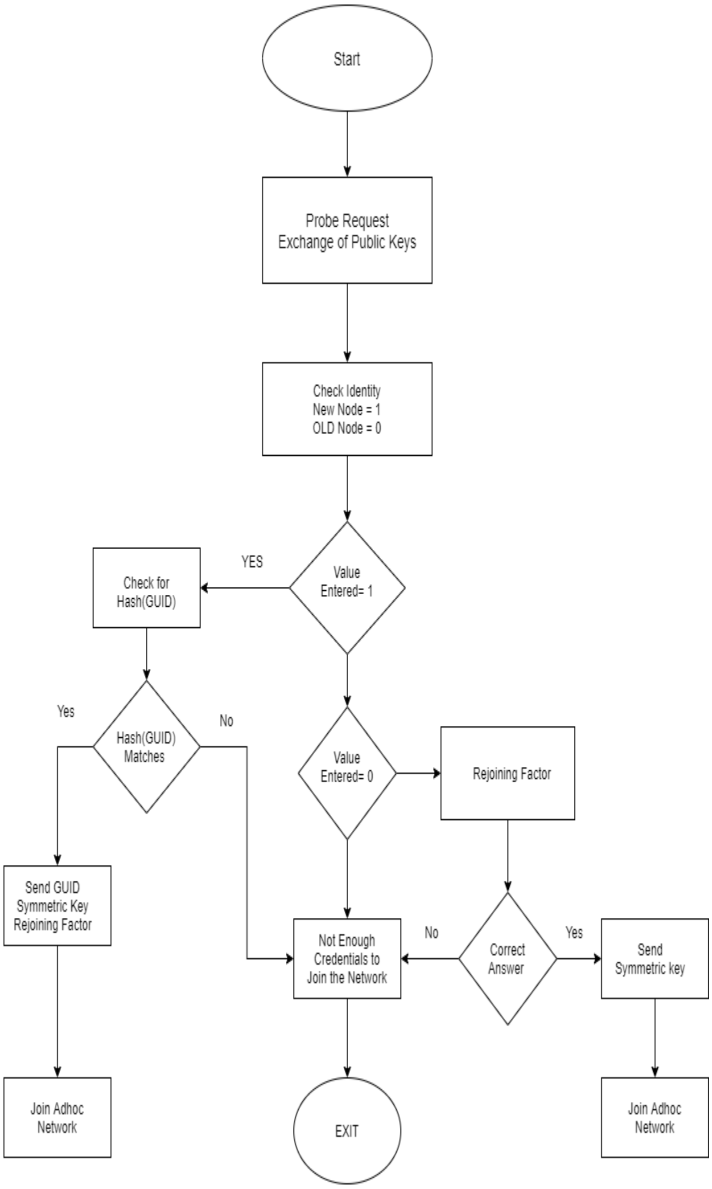

Fig. 1 Decision Flowchart of Proposed System.

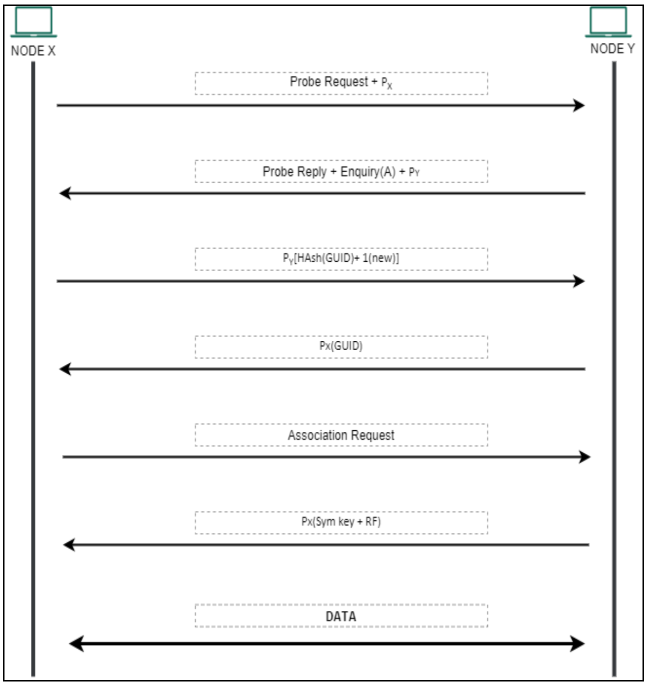

Fig. 2 Timing Diagram for Scenario 1.

2) Scenario 2: For old Nodes

Whenever a node gets disconnected from the ad-hoc network and wants to reconnect, it considers X as an old node and wants to reconnect to the network via Node Y. Node X sends a probe request containing RF, encrypted with PY. In return node Y sends an encrypted frame PX containing a symmetric key for secure transmission as depicted in Figure 3.

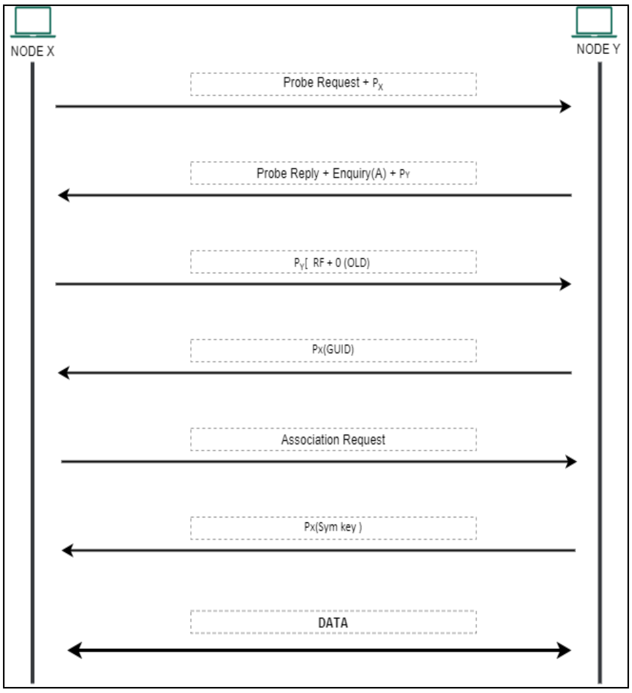

Figure 3 Timing Diagram for Scenario 2.

In the proposed framework authentication of a node is done using asymmetric keys and hash functions to ensure both parties are legitimate. After successful authentication of nodes symmetrical key encryption is used to secure communication among nodes.

The pseudo code for the presented approach is given as:

```
X→Probe request + $P_X$
Y→A + $P_Y$
X→ $P_Y$ [ Hash(GUID) + A]
If A=1 (New Node)
Then
X→ $P_Y$ [ Hash(GUID) + 1]
If
$[Hash(GUID)]_X = [Hash(GUID)]_Y$
Authenticating the incoming node (X)
then
Y → $P_X$(GUID)
If
$[GUID]_X = [GUID]_Y$
Authenticating the already existing node (Y)
Then
Authentication successful
Association phase
Y→Sym Key +RF
X → Sym Key [Data]
End
End
Elseif A=0 (OLD Node)
Then X→ $P_Y$ [ RF+0]
IF RF is authentic then
Authenticating the incoming node (X)
Y → $P_X$(GUID)
If
$[GUID]_X = [GUID]_Y$
Authenticating the already existing node (Y)
Then
Authentication successful
Association phase
Y→Sym Key +RF
X → Sym Key [Data]
End
End
End
End.
```

4. Simulation and Results.

The framework was simulated using the open-source network simulator NS-2. Considering the constrained nature of the MANet nodes, we have implemented efficient, lightweight protocols on the framework. PHOTON-128/16/16 is used as a hash function [27]. Elliptic Curve Cryptography (ECC-128) is used to generate asymmetric keys as it is well suited for power-constrained devices [28]. PRESENT-128, an energy-efficient block cipher is used for data encryption [28]. In the framework, GUID validates the node that wants to join the ad-hoc network. The Hash function Validates the node already present in the network and symmetric key encryption ensure the security of data during transmission. Table 2 shows the configuration of the simulator.

Table.2 Simulator Configuration

Tool	NS-2
No of nodes	2
Simulation Area	500m*500m
Routing protocol	DSDV
Channel	Wireless
Antenna Model	OmniAntenna
MAC Type	Mac/802_11
Interface queue type	Queue/DropTail/PriQueue

Table 3 Initial Connection Setup

Send/ Receive	Time	Node	Agent/ Routing	Payload Type	Packet size
s	0.050000000	0	AGT	tcp	40
r	0.050000000	0	RTR	tcp	40
s	0.050000000	0	RTR	DSDV	48
r	0.056524311	1	RTR	DSDV	48
s	0.056524311	1	RTR	DSDV	44
r	0.056524311	0	RTR	DSDV	44
s	0.056524311	0	RTR	tcp	40
r	0.058000000	1	AGT	tcp	40

In this framework, communication between the new node and the existing node takes place with the help of TCP and DSDV packets. DSDV communication takes only 6ms as starts at 50ms and stops at 56ms and TCP communication takes 8ms i.e. initial connection establishment is done in 14ms. Table 3 shows the initials connection establishment process.

Table 4 Simulation parameters for data with sequence number 60

Send/ Receive	Time	Node	Agent/ Routing	Payload Type	Packet size	Seq No
s	0.354739226	0	AGT	tcp	1040	[60 0]
r	0.354739226	0	RTR	tcp	1040	[60 0]
s	0.354739226	0	RTR	tcp	1040	[60 0]
r	0.530926941	1	AGT	tcp	1040	[60 0]
s	0.530926941	1	AGT	ack	40	[60 0]
r	0.530926941	1	RTR	ack	40	[60 0]
s	0.530926941	1	RTR	ack	40	[60 0]
r	0.613373956	0	AGT	ack	40	[60 0]

Table 5 Simulation Parameters for sequence number 110

Send/ Receive	Time	Node	Agent/ Routing	Payload Type	Packet size	Seq No
s	3.693174837	0	AGT	tcp	1040	[110 0]
r	3.693174837	0	RTR	tcp	1040	[110 0]
s	3.693174837	0	RTR	tcp	1040	[110 0]
r	3.868351899	1	AGT	tcp	1040	[110 0]
s	3.868351899	1	AGT	ack	40	[110 0]
r	3.868351899	1	RTR	ack	40	[110 0]
s	3.868351899	1	RTR	ack	40	[110 0]
r	3.959434851	0	AGT	ack	40	[110 0]

The information obtained from table 4 and table 5 depicts that the average time for a single TCP phase is approximately 260ms. Using the given information, we can calculate the total time for scenario 1 and 2. Scenario 1, uses six iterations of TCP life cycle, so the total time for a new node to join the networks is approximately 1578ms. Also, the time taken for encrypting and decrypting is 200ms and 300ms, respectively [29]. So, the total time taken by a new node to join the network is 3538ms. Similarly, the total time taken by the old nodes to reconnect to the network is 3078ms. The comparison of time taken by the new and old nodes to join the network is depicted in Figure 4.

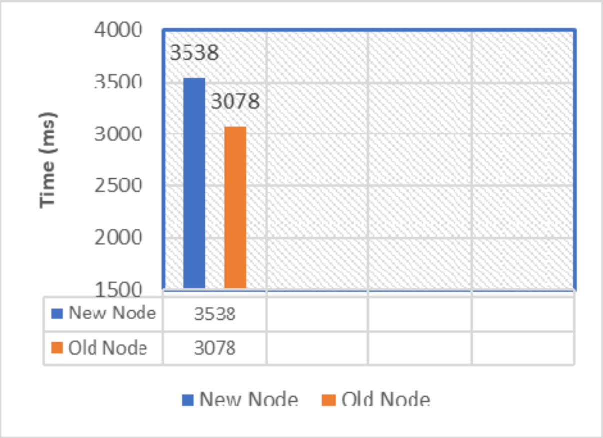

Figure 4 Comparison of time taken to join the Adhoc network.

5. Conclusion

Security is one of the most important concerns that will affect the overall performance of the MANets. In this research work, we proposed a secure framework for the authentication of ad-hoc nodes. The framework presented in this study does not require the central authorization server to authenticate the nodes. Instead, a distributed authentication mechanism is used. The proposed system makes use of lightweight hybrid encryption techniques to validate both parties.

References

[1]. Mishra, A., & Nadkarni, K. M. (2003). Security in wireless ad hoc networks. In The handbook of ad hoc wireless networks (pp. 499-549).

[2]. Luo, X., Chan, E. W., & Chang, R. K. (2006, April). Vanguard: a new detection scheme for a class of TCP-targeted denial-of-service attacks. In 2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006 (pp. 507-518). IEEE.

[3]. Raghavendran, C. H. V., Satish, G. N., & Varma, P. S. (2013). Security challenges and attacks in mobile ad hoc networks. International Journal of Information Engineering Electronic Business, 5(3), 49-58.

[4]. Tomić and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1910-1923, Dec. 2017, doi: 10.1109/JIOT.2017.2749883.

[5]. Fox, A., & Gribble, S. D. (1996, November). Security on the move: indirect authentication using Kerberos. In Proceedings of the 2nd annual international conference on Mobile computing and networking (pp. 155-164).

[6]. Pirzada, A. A., & McDonald, C. (2004, January). Kerberos assisted authentication in mobile ad-hoc networks. In Proceedings of the 27th Australasian conference on Computer science-Volume 26 (pp. 41-46).

[7]. Vijendran, A. S., & Gripsy, J. V. (2014, July). Enhanced secure multipath routing scheme in mobile adhoc and sensor networks. In Second International Conference on Current Trends In Engineering and Technology-ICCTET 2014 (pp. 210-215). IEEE.

[8]. Stoleru, R., Wu, H., & Chenji, H. (2011, October). Secure neighbor discovery in mobile ad hoc networks. In 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems (pp. 35-42). IEEE.

[9]. Mangrulkar, R. S., & Atique, M. (2010, December). Trust based secured adhoc On demand Distance Vector Routing protocol for mobile adhoc network. In 2010 Sixth International conference on Wireless Communication and Sensor Networks (pp. 1-4). IEEE.

[10]. Cho, J. H., Chen, R., & Chan, K. S. (2016). Trust threshold based public key management in mobile ad hoc networks. Ad Hoc Networks, 44, 58-75.

[11]. Li, J. S., & Yang, C. F. (2009, October). Quantum communication in distributed wireless sensor networks. In 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (pp. 1024-1029). IEEE.

[12]. Govindan, K., & Mohapatra, P. (2011). Trust computations and trust dynamics in mobile adhoc networks: A survey. IEEE Communications Surveys & Tutorials, 14(2), 279-298.

[13]. Fulare, R. P., & Sakhare, A. V. (2014, April). Efficient sensor node authentication in wireless integrated sensor networks using virtual certificate authority. In 2014 Fourth International Conference on Communication Systems and Network Technologies (pp. 724-728). IEEE.

[14]. Shim, K., Do, T. N., & An, B. (2018, February). A physical layer security-based routing protocol in mobile ad-hoc wireless networks. In 2018 20th International Conference on Advanced Communication Technology (ICACT) (pp. 417-422). IEEE.

[15]. Prakruthi, M. K., & Varalatchoumy, M. (2011). Detecting malicious beacon nodes for secure localisation in distributed wireless networks.

[16]. Kumar, S., Goyal, M., Goyal, D., & Poonia, R. C. (2017, December). Routing protocols and security issues in MANET. In 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS) (pp. 818-824). IEEE.

[17]. Waraich, P. S., & Batra, N. (2017, September). Prevention of denial of service attack over vehicle ad hoc networks using quick response table. In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC) (pp. 586-591). IEEE.

[18]. Usmani, J., Kumar, R., & Prakash, J. (2017, January). A survey on secure gateway discovery in MANET. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 362-368). IEEE.

[19]. Soni, M., & Joshi, B. K. (2016, November). Security assessment of routing protocols in Mobile Adhoc Networks. In 2016 International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-5). IEEE.

[20]. Gupta, D. S., Islam, S. H., & Obaidat, M. S. (2019, August). A Secure Identity-based Deniable Authentication Protocol for MANETs. In 2019 International Conference on

Computer, Information and Telecommunication Systems (CITS) (pp. 1-5). IEEE.

[21]. Hamamreh, R. A., Ayyad, M., & Jamoos, M. (2019, October). RAD: Reinforcement Authentication DYMO Protocol for MANET. In 2019 International Conference on Promising Electronic Technologies (ICPET) (pp. 136-141). IEEE.

[22]. Junnarkar, A. A., Singh, Y. P., & Deshpande, V. S. (2018, October). SQMAA: Security, QoS and Mobility Aware ACO Based Opportunistic Routing Protocol for MANET. In 2018 4th International Conference for Convergence in Technology (I2CT) (pp. 1-6). IEEE.

[23]. Verma, U. K., Kumar, S., & Sinha, D. (2016, March). A secure and efficient certificate based authentication protocol for MANET. In 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1-7). IEEE.

[24]. P. Yadav and M. Hussain, "A secure AODV routing protocol with node authentication," 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2017, pp. 489-493, doi: 10.1109/ICECA.2017.8203733.

[25]. Dilli, R., & Reddy, P. C. S. (2016, October). Implementation of security features in MANETs using SHA-3 standard algorithm. In 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) (pp. 455-458). IEEE.

[26]. Usha, M. K., & Poornima, A. S. (2016, March). Node-to-node authentication protocol to prevent black hole attack in AODV. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 133-136). IEEE.

[27]. Guo, J., Peyrin, T., & Poschmann, A. (2011, August). The PHOTON family of lightweight hash functions. In Annual Cryptology Conference (pp. 222-239). Springer, Berlin, Heidelberg.

[28]. Jadhav, S. P. (2019). Towards Light Weight Cryptography Schemes for Resource Constraint Devices in IoT. Journal of Mobile Multimedia, 15(1), 91-110.

[29]. Obaidur Rahaman, Data and Information Security in Modern World by using Elliptic Curve Cryptography, Computer Science and Engineering, Vol. 7 No. 2, 2017, pp. 29-44. doi: 10.5923/j.computer.20170702.01.