ISSN 2394-739X

IJRSET

International Journal for Research in Science Engineering and Technology

SURVEY ON SECURE ROUTING PROTOCOLS ON MOBILE AD-HOC NETWORK

[1] M. JAGANATHAN, [2] Dr. R. NAGARAJ
[1] RESEARCH SCHOLOR, [2] ASSOCIATE PROFESSOR
[1, 2] PG AND RESEARCH DEPARTMENT OF COMPUTER SCIENCE
[1, 2] KAAMADHENU ARTS AND SCIENCE COLLEGE
[1, 2] SATHYAMANGALAM, TAMILNADU, INDIA.

ABSTRACT: Mobile Ad-hoc network (MANET) is a self designing, multi hop wireless network. Security in mobile AD-HOC network is a major test on the grounds that there is no concentrated power which can regulate the individual nodes working in the network. The attacks can emerge out of inside the network and furthermore from the outside. This paper overviews the secure routing protocol in MANET, and furthermore talking about by and by proposed technique for alleviating those assaults. In the routing protocol of the MANET while sending data packets to different nodes, some middle of the road node remove valuable information packets and can't advance the bundle to the following node. Some node may adjust the substance of packets during the data transmission meeting. With the goal that any one node can control the first data. This paper likewise gives a short outline and correlation of different protocols available for secured routing in MANET.

Keywords: [Ad-hoc Network, Protocol, Routing, Security, Attacks, MANET.]

1. INTRODUCTION

A mobile ad hoc network (MANET) is a network of remote mobile devices. A node can be a PC, a PDA, a mobile telephone, or any mobile device with the capacity to speak with different devices. The topology of the network continues changing after some time as nodes may move about, some new nodes join the network, or some different nodes separate themselves from the network. The network is made, overseen, and sorted out absolutely by the nodes themselves without the help of any brought together outsider or fixed framework. Thus, participation of the nodes among themselves is the stage on which this network is assembled. A node not just uses the network for speaking with different nodes, yet in addition bolsters the network by performing routing capacities. A node that needs to speak with another node which isn't inside its correspondence go takes the assistance of the middle of the way nodes to transfer its message. MANETs have unmistakable advantages over traditional networks in that they can without much of a stretch be set up and destroyed, aside from giving adaptability as the nodes are not fastened. Figure 1 gives a communication among MANET.

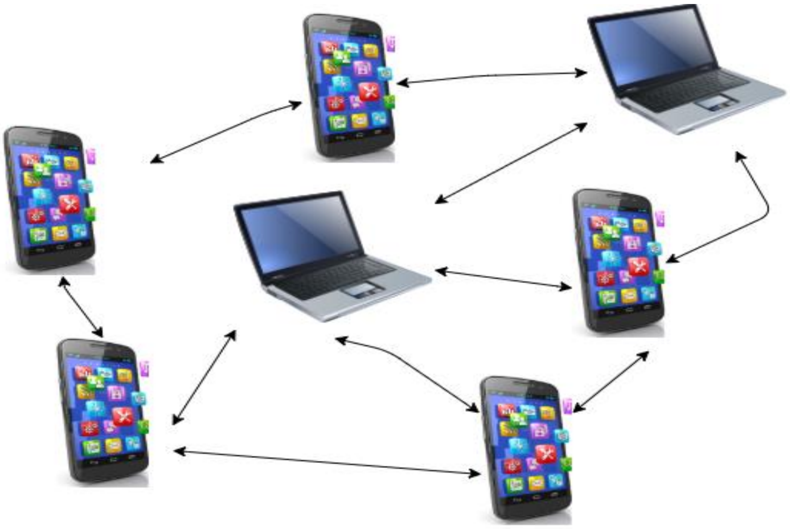

Figure 1: Communication among MANET

2. PROBLEMS IN SECURING THE ROUTING PROTOCOLS

Securing the routing protocols for ad hoc networks is a difficult assignment because of its one of kind qualities. A short conversation on how the qualities causes' trouble in giving security in ad hoc wireless network is given below.

1) Shared radio channel: Unlike the wired networks where a different committed transmission line can be given between a couple of end clients, the radio channel utilized for correspondence in ad hoc networks is broadcast in nature and shared by all nodes in the network. Data transmitted by a node is gotten by all the nodes inside its direct

2) Transmission range: Malicious node can without much of a stretch acquire data being transmitted in the network. Insecure condition in which MANET are commonly utilized may not be constantly secure, for instance, The protection war zone. In such condition, nodes may move all through threatening and insecure hostile area, where they would be exceptionally defenseless against security attacks.

3) Lack of central authority: infrastructure based wireless networks it is conceivable to screen the network traffic through switches or base stations and actualize security systems at those focuses. Since MANET don't have any such essential issues, these components can't be appropriate to them.

4) Lack of association rules: In MANET, since nodes can leave or join the network anytime of time, if no legitimate confirmation system is utilized for associating nodes with the network gatecrashers can without much of a stretch join the network and complete attacks.

5) Limited accessibility of resources: Resources, for example, data transfer capacity (bandwidth), battery power and computational force are alarm in ad hoc networks. Henceforth, it is hard to actualize complex cryptography-based security mechanisms in such networks.

3. ROUTING ATTACKS IN MANETS

Due to characteristics of mobile ad-hoc networks, MANETs are more defenseless attacked than wired networks. We can recognize two head classes of attacks: passive and active attacks. A passive attack doesn't upset the activity of the protocol, however endeavors to tune in to important information in the rush traffic. Instead, an active attack disturbs the activity of the protocol so as to degrade the network execution, increase unapproved get to, and confine accessibility.

PASSIVE ATTACKS	ACTIVE ATTACKS
Snooping	Wormhole
Eavesdropping	Black hole
Traffic Analysis	Gray hole
Monitoring	Information disclosure
	Resource consumption
	Routing attacks

Table 1: Network Security attacks in MANET

4. DIFFERENT SECURE ROUTING PROTOCOLS

For the secure routing protocol first need appropriate authentication need to digital signature of each and every authenticated nodes. It additionally need to variable information of the control packets. It likewise frequently supplemented with the utilization of single direction hash capacities. Recognize wormhole and the passage. These routing plans give authentication administrations which guard against modification and replaying of routing control messages and uses distinctive cryptographic primitives for giving secure routing.

4.1 BASIC ROUTING PROTOCOLS

This protocol kept up by the starting node hashing the messages and marking the came about message digest, which is confirmed by the beneficiaries of a route request, by registering the hash of a message utilizing the settled upon hash function. The advantage is that the protocol can battle outside attacks by checking for the genuineness. The advantage of this protocol is that it expands the ICMP switch revelation bundle configuration to incorporate the MAC and IP address of the sender, and authentication information that can be utilized to check the broadcast beacon. Yet, its disadvantage is that it expects nodes to have shared secret keys for generating message authentication codes which are utilized to authenticate the routing control messages and the plan depends on the supposition that the nodes in the network commonly trust one another and it utilizes public key cryptography for giving the security administrations.

1. Elbasher Elmahdi, Seong-Moo Yoo and Kumar Sharshembiev (2018) et.al proposed another way to deal with give solid and secure data transmission in MANETs under conceivable blackhole attacks dependent on on ad hoc on-demand multipath distance vector (AOMDV) protocol and homomorphic encryption scheme for security. Our proposed conspire depends on ad hoc on-demand multipath distance vector (AOMDV) protocol for discovering active transmission paths. Authors researched the security of AOMDV protocol, a multipath extension of the AODV routing protocol against black hole attacks. In the wake of finding the routes between a source and a destination node, a message is part into numerous parts and each part is encrypted utilizing homomorphic encryption technique before the sender transmits a part of the message to the destination. Here, malicious nodes might be contained in the route and may make black hole attacks. The issue of the attacks in the AOMDV protocol is addressed in this paper. In this way, their plan isn't an intrusion detection or intrusion isolation system, but it is an intrusion avoidance system from malicious nodes.

Merits

- The performance of the proposed scheme is stable but that of AOMDV is found to be degrading with the intrusion of malicious nodes in the network.
- The proposed plan to guarantee and assurance the conveyance of the packet to the

objective is high with numerous active paths in each gathering of the network.

Demerits

- It won't decline end-to-end delay to apply to the emergency applications in MANETs.

2. Ranjit Kumar, Sachin Tripathi and Rajeev Agrawal (2018) et.al a Secure HandShaking AODV Routing Protocol (SHS-AODV). The securing of the diverse proposed Routing Protocols (RPs) has shown that the characteristic ad hoc network, for example, rapidly changing topologies and nonappearance of structure, present further issues with the adequately jumbled issue of secure routing. In the interim, as standard RP, Ad-hoc on-request separation vector (AODV) RP has been related thoroughly in MANET. Beginning at now, how to upgrade the transmission execution and improve security are the two essential perspectives in AODV's exploration field. To improve the wellbeing of such network, the strategy proposed directly here is securing sure about RP, AODV through utilizing RSA Algorithm and Symmetric Encryption algorithm AES. This secures the data just as jam the secrecy, trustworthiness, and validness. Our examination exhibits that none of the proposition of secure RPs can satisfy all security goals

Merits

- The proposed strategy SHA-AODV RP, the network execution improves by showing throughput, vitality and bundle conveyance proportion (PDR).
- The SHS-AODV protocol is reasonable for the conditions, which are delay-inhumane, yet have a high-security essential.

Demerits

- Forgery Attack is decreased by their proposed technique SHS-AODV. Here the fake packet can be detected by the source and destination nodes.

3. Rajat Kishor Varshney , Dr. Anil Kumar Sagar (2018) et.al proposed an Improved AODV Protocol to Detect Malicious Node in Ad hoc Network. The motivation behind this paper is to identify maliciousnode and to expel them to secure correspondence among source and destination, and for security of the network course they use RSA key exchange algorithm. This algorithm is a asymmetric encryption algorithm, it tends to be utilized with digital signatures, key exchange and encryption. In this paper the nodes gets false information's from that point neighbors is customized to take a gander at neighbor nodes as adulterated node, to recognize and evacuate them. In this Paper authors utilized a system when the wireless network makes the numerous nodes, right off the bat watch that whether this network contain any adulterated node or not. On the off chance that this network contains any malicious node, at that point authors need to expel it to secure our network. In the event that authors get any node which get false information from its neighbor, this node is considered as malignant node, at that point this node transmit bogus information to its other neighbor's nodes and authors need to expel this noxious node for quality and security reason. The nodes in the wireless network are distinguished based on their unique Identification number.

Merits

- Improved Ad hoc On-Demand Distance Vector is applied to pull out malicious node.
- The RSA key exchange algorithm is used to secure the wireless network to improve security mechanism has been finished twice.

Demerits

- Shortest path may be lost due to traffic during the path discovery process.

4.2 TRUST BASED ROUTING PROTOCOLS

Trust is a value that can calculated on the based on nodes activity when it required. Trust used to keep from different attacks like wormhole, black hole, Dos, selfish assault and so on. Trust can be executed in different manners, for example, by reputation, from opinion of nodes etc. This routing security schemes which fall in this class allocate quantitative qualities to the nodes in the network, in view of watched conduct of the nodes being referred to. The trust values are then utilized as additional measurements for the routing protocols. The advantage is that it is powerful against individual attackers and fit for adjusting its degree among nearby and network wide topology discovery. It can likewise work well in networks where the topology and membership is changing every now and again.

4. Sajyth RB and Sujatha G (2018) et.al proposed Reliable Bee Clustering Routing Protocol in MANET . ECC (Elliptical Curve Cryptography) is coordinated with the Bee clustering way to deal with give a vitality productive and secure data delivery system. Despite the fact that it guarantees data confidentiality, data reliability is as yet questionable, for example, data dropping attack, Black hole attack (Attacker router drops the data without forwarding to destination). In such cases the procedure of catching is used by the neighbor routers and the parcel sending insights are estimated dependent on the proportion between the got and sent packets. The presence of attack is detected if the packet sending proportion is poor in the network which paves a way to the alternate path identification for a reliable data transmission.

Merits

- Thus proposed approach guarantees both reliability and data confidentiality.
- To improve energy efficiency of routing energy based CH is used for routing that follows bee colony optimization algorithm.

Demerits

- The proposed protocol is low in control message overhead.

5. S. Karthick, S. Perumal Sankar and Y.P. Arul Teen (2018) proposed Trust-Distrust Protocol for Secure Routing in SelfOrganizing Networks. In this paper, authors develop a novel protocol for the secure routing in SONs, which is named as Trust-Distrust Protocol (TDP). According to the proposed protocol, the routing is done in four phases. In the underlying stage topology the board utilizing an improved column k-implies algorithm. The subsequent stage is Link Quality Appraisal (LQA) in light of the wellness of nodes. The third stage is grading, in which a grade point is distributed to each node dependent on LQA. In the last stage the secure way for the routing is resolved dependent on the grade point. The proposed protocol is tried in one of the significant sorts of SONs, similar to MANET utilizing the MATLAB look into device. At last the proposed protocol outflanks the exhibition of the current routing techniques.

Merits

- The proposed system has improved average success ratio and reduced energy consumption.
- It proves that the security of the proposed system is achieved by this enhance success ratio.
- The overall proposed system become become extraordinary compared to other decision for routing in SON with high security and diminished vitality utilization.

Demerits

- The proposed protocol is low quality of data transmission while routing.

6. K.Dhanya, Dr.C.Jeyalakshmi, and A.Balakumar (2019) et.al proposes an inspection on Trust Based Routing protocols to protect Internet of Things directing to authorize dependability and privacy amid to direction-finding procedure in inaccessible systems. Trust is an imperative part of Internet of Things (IOT). It empowers elements to adapt to vulnerability and roughness brought about by the completely opportunity of different devices. In Mobile Ad-hoc Network (MANET) have moves every now and again in any bearing, with the goal that the topology of the network likewise changes as often as possible. No particular algorithm is utilized for routing the packets. Packets/data must be directed by transitional nodes. It is procumbent to various events ease. There are different ways to deal with process trust for a node, for example, fluffy trust approach, trust administration approach, half and half methodology, and so on. Adaptive Information Dissemination (AID) is a system which guarantees the packets in a particular transmission and it examination of is there any attacks by programmers. It includes of guaranteeing the packet count and route detection among source and destination with confided in way. Trust estimation reliant on the particular condition or setting of a center point, by sharing the setting information onto substitute centers in the system would offer a predominant response for this issue.

Merits

- Attack patterns, Throughput and AP Discovery are high.
- Proposed System (AID Protocol) is elite in route discovery and discovery ratio.

Demerits

- Node mobility and link failure are major concerns in MANETs.

4.3 INCENTIVE BASED ROUTING PROTOCOLS

In ad hoc networks, devices need to coordinate. Autonomous devices will in general swear off collaboration. Incentive schemes have been proposed as a means of fostering cooperation under these circumstances. So as to work viably, incentive schemes should be painstakingly custom fitted to the characteristics of the cooperation protocol they should bolster. These routing schemes actualized utilizing credits that are given to nodes that participate and forward packets. Thus network administrations, for example, routing is given distinctly to those nodes that have great credit. On the off chance that a node at a troublesome area may not get enough packets to advance and in this way may always be unable to get credits to advance its own packets.

7. K RAMA ABIRAMI1 and M G SUMITHRA (2018) et.al proposed Neighbor Credit Value based AODV (NCV-AODV) routing algorithm for the detection of selfish behavior which avoids such false detection. The proposed thought is actualized in Ad hoc On Demand Distance Vector (AODV) routing protocol and a extensive analysis on the presentation of the proposed detection mechanism against the selfish behavior of some MANET nodes are conducted. The greater part of the past "credit based" location techniques will work by hearing or catching the neighbor data transmissions. In this way, if a neighboring node which isn't effectively sending or accepting any data might be misclassified as a malicious node. To defeat this issue, the proposed strategy will recreate some fake data traffic from such inert veritable nodes to forestall them set apart as malicious.

Merits

- The proposed methods effectively identifying the selfish neighbor nodes and avoid sending packets through them which obviously improved the overall performance.
- It will resolve the credit value of neighbors in an efficient way and provide better performance without any noticeable increase in detection overhead.

Demerits

- On the off chance that a node at a negative area may not get enough packets to advance and accordingly may always be unable to get credits to advance its own packets.

4.4 DETECTION AND ISOLATION BASED SECURE ROUTING SCHEME

This protocol can identifies flooding, black hole, gray hole, wormhole and blackmail attacks. On detection the protocol takes prompt activities to boycott these nodes from the network, in this manner diminishing the quantity of malicious nodes in a network, henceforth improving the different QoS parameters. This protocol distinguishes and confines making misbehaving nodes in MANET. It is an upgrade of DSR routing and dependent on choice of selfish and unselfish nodes. The advantage is that the trust and routing computation process is assessed by understanding, perception and conduct of different nodes, present in the network. This protocol can viably recognize selfish nodes and isolate wormhole nodes that drop packets.

8. Taku Noguchi, Mayuko Hayakawa (2018) et.al propose a new threshold-based black hole attack prevention method using multiple RREPs. The proposed strategy for defense against a black hole attack in AODV. The proposed strategy permits numerous RREPs to be sent for a similar Route REQuest (RREQ) packet. Different RREPs help both the source node and the middle of the road nodes on the potential path for the destination node to gather a ton of information about the path. After accepting a RREQ packet, every node dynamically calculates the average of RREP sequence numbers which are generated by the same node from a current RREP and past received RREPs. The proposed strategy considers the generator node of the RREP which has a higher normal RREP succession number than the edge an incentive as a dark opening node. This limit is determined from the normal of RREP arrangement numbers for a similar destination node. To research the exhibition of the proposed technique, it was contrasted and a current secure AODV protocol. To research the exhibition of the proposed strategy, authors contrasted it and existing techniques.

Merits

- The proposed method beats existing methods from the standpoints of packet delivery rate, throughput, and routing overhead.

Demerits

- It can't fit with different network sizes and node mobilities.
- The proposed method not improve the packet delivery rate with the larger number of nodes

9. ALY M. EL-SEMARY1, and HOSSAM DIAB (2019) et.al proposes a secure MANET routing protocol called BP-AODV to overcome the security breaches related to the SAODV protocol along with the original AODV protocol. In addition, the BPAODV can secure against a helpful blackhole assault propelled during the routing procedure and gatekeepers against the blackhole assault that may occur during the sending procedure. The BP-AODV is created by broadening the usefulness of the AODV protocol alongside using the riotous guide highlights. The exploratory outcomes guarantee that the BP-AODV protocol is more secure than the SAODV protocol and can successfully battle the blackhole assault accomplished by a malicious node or agreeable malicious nodes during the routing procedure. The BP-AODV is actualized utilizing the notable network test system form 2 (NS2) and thought about against the AODV, SAODV, and PCBHA protocols. The outcomes likewise uncover that the BP-AODV can emphatically make preparations for the blackhole assault that happens during the forwarding process.

Merits

- The BP-AODV protocol is effective in thwarting blackhole attack that might be occurred in various situations.

Demerits

- Its drawback is that it cannot detect multiple black hole attacks and the control messages have been expanded.

10. Milan Kumar Dholey and G. P. Biswas (2018) et.al proposed DSR protocol for restricting a malicious node to misguide MANET routing. The malicious node may send RREP control message to the source and occupied source to send the data packet in wrong destination by sending diverse path information. Here, from their propose algorithm even a malicious node may introduce into the network and act as a neighbor in spite of the fact that before data correspondence source can decide about the original receiver and stop transmitting data. For structuring our algorithm authors apply existing PGP encryption program. Our thought is that, climate source can distinguished where the data is sending then data preoccupation can be forestalled. Along these lines, data preoccupation won't happen and DSR routing protocol is in some stretch out is increasingly secure as indicated by their proposal algorithm.

Merits

- The proposed DSR routing protocol is profoundly secured.

Demerits

- A malicious node and get RREQ control message but according to our proposal they may not get control over the data transmission.
- If group attack is done by the malicious nodes so some security issues will emerge.

11. Adwan Yasin and Mahmoud Abu Zant (2018) et.al introduced a smart black-hole detection and isolation technique that should be considered in constructing and developing any black-hole fghting protocols or techniques. The proposed TBBT comprises both timers and baiting techniques in order to enhance black-hole detection capability while preserving Troughput, End-toEnd Delay, and Packet Delivery Ratio. Te proposed technique consists of two phases: Baiting and Nonneighbor Reply. In Baiting phase each node has a bait-timer, the value of the timer is set randomly to B seconds, and each time the timer reaches B it creates and broadcasts a bait request with a randomly generated fake id. Contingent upon the characteristic conduct of a dark gap node when it gets any course demand it reacts with an answer asserting that it has the best path regardless of whether it doesn't exist. At the point when the dark opening gets the teased solicitation it sends an answer to the source node asserting that it has a course; when the source node receives the answer it quickly considers the node which reacted as a dark gap and adds it to the dark gap list since it professed to have a course to a phony node. The recreation aftereffects of the proposed procedure demonstrated that the End-to-End Delay, Throughput, and Packet Delivery Ratio are near the local AODV.

Merits

- The proposed technique demonstrated that the End-to-End Delay, Troughput, and Packet Delivery Ratio is good.

Demerits

- Implementation is proficient way is difficult and often requires highly skilled labours and engineers.

CONCLUSION

In this paper, we have presented a review of problems in securing the routing protocols, attacks on physical, data and network layers, and also provide survey on different secure routing protocol. Various routing protocols discussed in the paper are very helpful and effective for new researchers to identify current issues for advance research. Numerous new routing protocols are proposed nowadays yet at the same time there is an open research issue what protocol shows best conduct in which circumstance. A lot of contribution has been made in this field and several merits and demerits also addressed.

REFERENCES

[1]. Elbasher Elmahdi, Seong-Moo Yoo and Kumar Sharshembiev (2018), "Securing Data Forwarding against Blackhole Attacks in Mobile Ad Hoc Networks", **DOI:** 10.1109/CCWC.2018.8301683, **Electronic ISBN:** 978-1-5386-4649-6, IEEE.

[2]. Ranjit Kumar, Sachin Tripathi and Rajeev Agrawal (2018), "A Secure HandShaking AODV Routing Protocol (SHS-AODV)", **DOI:** 10.1109/RAIT.2018.8389029, **Electronic ISBN:** 978-1-5386-3039-6, IEEE.

[3]. Rajat Kishor Varshney , Dr. Anil Kumar Sagar (2018), "An Improved AODV Protocol to Detect Malicious Node in Ad hoc Network", **DOI:** 10.1109/ICACCCN.2018.8748359, **DOI:** 10.1109/ICACCCN.2018.8748359, IEEE.

[4]. Sajyth RB and Sujatha G (2018), "Design of Data Confidential and Reliable Bee Clustering Routing Protocol in MANET", **DOI:** 10.1109/ICCCI.2018.8441217", **Electronic ISBN:** 978-1-5386-2238-4, IEEE.

[5]. S. Karthick, S. Perumal Sankar and Y.P. Arul Teen (2018), "Trust-Distrust Protocol for Secure Routing in SelfOrganizing Networks", **DOI:** 10.1109/ICETIETR.2018.8529016, **Electronic ISBN:** 978-1-5386-5744-7, IEEE.

[6]. K.Dhanya, Dr.C.Jeyalakshmi, and A.Balakumar (2019), "A Secure Autonomic Mobile Ad-hoc Network based Trusted Routing Proposal", **DOI:** 10.1109/ICCCI.2019.8822012, **Electronic ISBN:** 978-1-5386-8260-9, IEEE.

[7]. K RAMA ABIRAMI1 and M G SUMITHRA (2018), "Preventing the impact of selfish behavior under MANET using Neighbor Credit Value based AODV routing algorithm", Sådhanå (2018) 43:60 Indian Academy of Sciences https://doi.org/10.1007/s12046-018-0803-4Sadhana(0123456789().,-volV)FT3](0123456789().,-volV)

[8]. Taku Noguchi, Mayuko Hayakawa (2018), "Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks", **DOI:** 10.1109/TrustCom/BigDataSE.2018.00082, **Electronic ISSN:** 2324-9013, IEEE.

[9]. ALY M. EL-SEMARY1 , and HOSSAM DIAB (2019), "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs based on Chaotic Map", **DOI:** 10.1109/ACCESS.2019.2928804, **Electronic ISSN:** 2169-3536, IEEE.

[10]. Milan Kumar Dholey and G. P. Biswas (2018), "Secure DSR Routing From Malicious Node by PGP Encryption", **DOI:** 10.1109/ICOEI.2018.8553857, **Electronic ISBN:** 978-1-5386-3570-4, IEEE.

[11]. Adwan Yasin and Mahmoud Abu Zant (2018), "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique", Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 9812135, 10 pages https://doi.org/10.1155/2018/9812135.

[12]. Gaini Sujatha and Md. Abdul Azeem (2015), "UOSHR: UnObservable Secure Hybrid Routing Protocol for Fast Transmission in MANET", https://doi.org/10.1007/978-3-319-13731-5_51, Print ISBN978-3-319-13730-8, SpringerLink.

[13]. S. Syed Jamaesha and · S. Bhavani (2018), "A secure and efficient cluster based location aware routing protocol in MANET", https://doi.org/10.1007/s10586-018-1703-4, Cluster Comput 22, 4179–4186 (2019).