International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Security Threat of MANET: A Comprehensive Architecture

Ravneet Kaur Sidhu, Ram Krishan

Abstract: ***Throughout security in Mobile Ad-Hoc Network is the most critical worry for the fundamental convenience of the structure. The openness of framework organizations, protection and trustworthiness of the data can be cultivated by ensuring that the security issues have been met. Considering the features like open medium, a rapid change in the topology, MANET experience the evil impacts of various attacks. The network may have to suffer in two scenarios due to intrusion. First, when a node of the current network is influenced by the intruder and second which the intruder is participating himself. In both the cases, the earnest aim of the intruder to drop maximum number of packets and to produce un-necessary delay which may further produces routing overhead. In order to mitigate the effects of the intrusion, a lot of researchers have contributed and has studied the nature of the intrusion. This paper illustrates some of the recent articles over different security breaches and their possible solutions.***

Keywords: MANETs, Security Attacks, DoS, Trust Aggregation, Trust Prediction.

I. INTRODUCTION

Mobile Ad hoc Network (MANET) comprises of numerous Mobile nodes with wireless correspondence that can communicate with one another with no physical foundation. Also called as foundation less system. Every node can play out the job of a host just as a switch. Henceforth the nodes, which are out of transmission range can be gotten to by directing through middle of the road nodes. Frequently, has in a MANETs work with constrained batteries and can wander uninhibitedly towards any heading at any speed. The power depletion of certain nodes and the versatility idea of nodes cause visit topology changes. Therefore, the path between nodes or gathering of nodes may change occasionally. The node which needs to transmit information packets first needs to find the course to the destination by utilizing course disclosure procedure of various routing mechanisms. There are two sorts of directing mechanisms, one is reactive or on demand routing, and another is proactive or table-driven routing. In Mobile specially appointed systems, a host may deplete its capacity or move away without giving any notification to its helpful nodes, causing changes in topology, and subsequently these progressions may essentially debase the presentation of the routing mechanism. So, the network should be found with longer lifetime and less changes. As the network comprises of number of wireless connections, its lifetime relies upon the existence time of nodes and individual connections. The network revelation without considering its lifetime prompts visit disappointment and along these lines to network disclosure. Thus the computational overhead of the directing convention increments impressively [1]. This paper contains ten areas. Segment I exhibit an overall review structure of set up and case setup. MANETs security purposes are talked concerning Section II followed by brief description about routing protocols and vulnerabilities mentioned in Section IV. Active and Passive attacks on MANETs is analyzed in Section V and Section VI. Security approach review in Section VII and Routing protocol also reviewed in Section VIII. In conclusion, discourses and finishing up comments are introduced in Section IX and X.

II. MOBILE AD HOC NETWORK AND ITS ISSUES

Mobile Ad hoc Networks (MANETs) generally depicts mobile system that envelops the wireless mobile nodes. These nodes compose themselves progressively in irregular and unpredictable topologies. In such a situation, a wireless framework which can convey data from a source to destination, thinking about the versatility of the nodes as a primary concern. It is in this way, in light of the fact that a node can get a packet of information that is sent inside its recurrence extend.

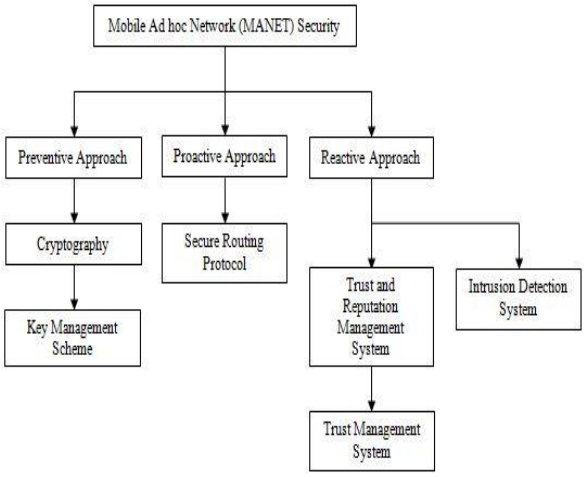

Fig.1. Overall Review Structure.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
Ravneet Kaur Sidhu*, Research scholar, Department of Computer Science, Punjabi University, Patiala, India Email: ravneetsidhu21@ymail.com
Ram Krishan, Assistant Professor, Department of Computer Science, Guru Kashi Collage, Punjabi University, Talwandi Sabo, India Email: ramkrishan@pbi.ac.in

Thus, when the nodes are mobile, the accepting node can move out of recurrence move wherever at any time. It enables individuals and gadgets to bury organize in zones with no previous correspondence foundation [2].

MANETs are self-consolidating networks where most or all of the nodes are mobile thus having a changing network topology. The nodes in a mobile ad hoc network act both as a host and a router making MANETs heterogeneous. Therefore, the most prominent issue that arises in MANETs is its security. The need of security can be described in terms of obtainability, reliability, privacy, validity, anonymity, authenticity.

III. ROUTING PROTOCOLS

Routing protocols can be categorized into proactive, reactive and hybrid protocols, contingent upon the routing topology [14].

- Proactive protocols are normally table-driven and distance-vector protocols, hence taking after numerous conventional protocols. In proactive protocols the hubs intermittently invigorate of the current routing data so every hub can promptly work with predictable and modern routing tables at whatever point there is information to be sent. The unadulterated proactive protocols don't suite ad hoc systems because of consistent and overwhelming control traffic conveyance between the hubs. Particularly in MANET systems there regularly needs to exist a few substitute ways to the goal for unwavering quality reasons, which causes visit trade of excess control data.
- Reactive or source-initiated on-demand protocols, in opposite, don't intermittently refresh the routing information - it is sent to the hubs just when required. A large number of the MANET routing protocols are on-demand driven for streamlining purposes. The inconvenience of the reactive protocols is that they generate huge outlay when the path is being resolved, since the paths are not advanced when required.
- Hybrid protocols can generally be considered the combination of both proactive and reactive methodologies. They work by switching between the two protocols. For example, table-driven protocols could be utilized among systems and on-request protocols inside the systems or the other way around. It appears that systems neither the proactive nor the responsive methodology is adequate, because of the referenced issues, so the half breed approach might be by and large the ideal choice. For instance, table-driven protocols could be used between networks and on-demand protocols inside the networks or vice versa. It seems that networks neither the pure proactive nor the reactive approach is sufficient, due to the mentioned problems, so the hybrid approach may be in general the optimal.

IV. VULNERABILITIES

Wireless medium is viewed as more presented to security attacks than wired connections because of its vulnerabilities. Since wireless medium is a spine of the MANETs, along these lines MANETs acquire every single highlights of wireless connections. These acquired vulnerabilities of wireless medium make the MANETs profoundly helpless in nature and a store for all term attacks. [3].

- *No Secure Boundaries:* In a wired system, intruder aims to get physical access to the system medium. They may even need to experience layers of firewall and portal. Be that as it may, in MANETs, it is anything but ∂difficult to access the system, provided the node is in recurrence range [4]. In this manner, MANETs don't give secure boundary.
- *Power and Reckoning Limitations:* Wired systems can get electric power supplies, yet on account of wireless system, there is limited power supply. In this way, any node in a system may act narrow minded, on the off chance that it has restricted power supply [4]. The battery once deployed can never be change throughout the entire lifetime.
- *Lack of Centralized Management Facility:* Ad-hoc systems don't have a focal component that is utilized for the executives, prompting some defenseless issues. The absence of brought together network apparatus makes the ID of packets a troublesome issue as it is difficult to check and control the traffic in a profoundly unique and enormous scale specially appointed system.
- *Supportiveness:* The basic supposition about routing algorithms in MANETs is that the nodes are helpful and non-malignant. Therefore, a malicious aggressor can without much of a stretch become a fundamental directing specialist and interfere with ordered activities by ignoring the convention details.

V. ACTIVE ATTACKS ON MANETS

Dynamic attacks are the attacks that are performed by the malicious nodes. Additionally, these nodes expend some vitality so as to play out the attacks. Dynamic attacks include a few changes of information or formation of bogus data. The accompanying attacks go under the classification of dynamic attacks:

- *Sink Holes:* An undermined node attempts to draw in the information to it, from every single neighboring node. The node listens stealthily on every one of the information that is being conveyed among its neighboring nodes. Sinkhole attacks can likewise happen on specially appointed systems, for example, AODV by utilizing procedures like boosting the arrangement number or limiting the hop check.

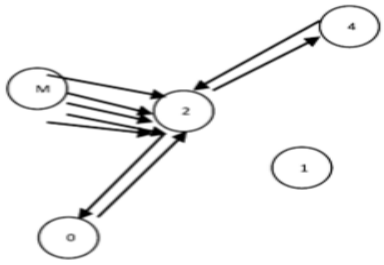

Fig.2. Denial of Service Attack.

- Denial of Service (DoS*):* The DoS attacks are performed by flooding some sort of system traffic to the objective.

This debilitates the preparing intensity of the objective and makes the administrations gave by the objective inaccessible. The disseminated idea of the administrations makes it illogical. Additionally, the portable systems are more helpless than the wired systems.

- Wormhole Attack: Wormhole attacks are of extreme danger to MANETs routing architecture. At the point when the invader records bundle at a spot, and diverts them to another area, routing is affected. This happens as a result of the redirection. Such incidents are nomenclature as wormhole attacks shown in Fig .3.

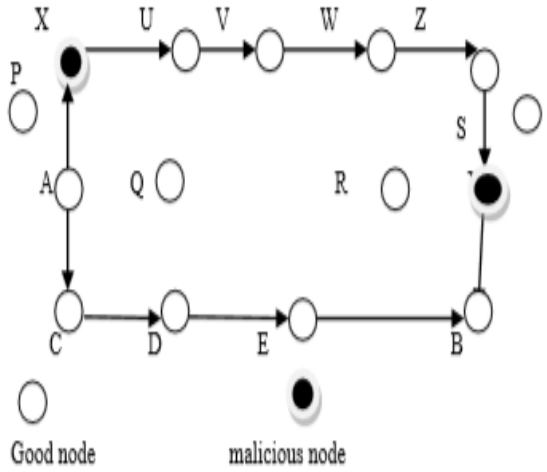

Fig.3. Scenario of Network while Wormhole Attack

- *Modification:* It influences the honesty of information. The aggressor changes the packet.
- *Spoofing:* Spoofing happens when a malevolent node imagines as some other node. It does as such to adjust the vision of the system topology that a blameless node can gather [4]. Satirizing is additionally called the man in the center. The aggressor accomplishes this, by indicating its IP as the IP of the node it needs to go about as.
- *Fabrication:* Attacks performed by producing bogus directing data, are creation. These are hard to recognize since they come as legitimate steering builds, particularly on account of mistaken. They guarantee that a neighbor can never again be reached.
- *Sybil Attack:* At the point when one node mimics a gathering of nodes, it is known as Sybil attack. This is an intricate attack as a node relies upon many middles of the road nodes for correspondence, thus there are excess calculations to guarantee the conveyance of information. Be that as it may, if a solitary malicious node can speak to numerous nodes; it gets less complex for the assailant.

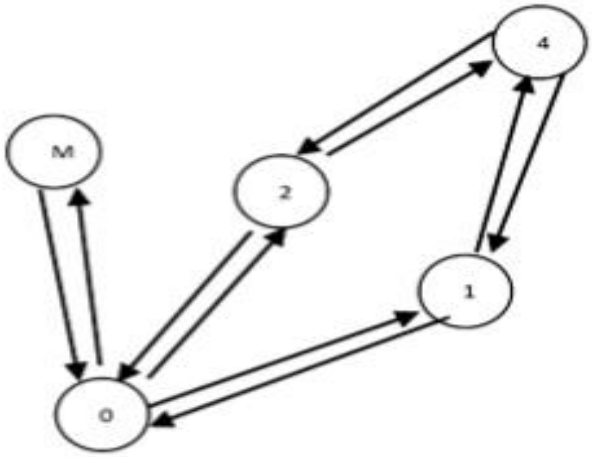

Fig.4. Scenario of Sybil Attack.

Presently, the goal nodes can't decipher the adjustment in bundles. Counterfeit proposals about the trustworthiness of a specific gathering can likewise be conveyed, consequently pulling in more rush hour gridlock to it.

VI. PASSIVE ATTACKS ON MANET

In passive attacks, the routing isn't disrupted. Significant data like node progression and system topology is gotten. The assailant's goal is to acquire data that is being transmitted. Uninvolved attacks are hard to recognize as they don't include any change of information. Coming up next are passive attacks.

A. Eaves Dropping

The goal of listening stealthily is to acquire some classified data during correspondence. The classified data may incorporate the area, open key, private key or even passwords of the nodes. It is significant that such information is kept escaped unapproved individuals.

B. Traffic Analysis

In this attack, the assailant examines the traffic, decide the area, inquire about what is transferred, distinguish the recurrence and length of message being traded. These data are utilized to foresee the idea of correspondence. All approaching and active traffic of system isn't changed.

C. Monitoring

The nodes are observed. The bundle exchanges and different exercises of the node are confirmed and examined.

VII. SECURITY REVIEW PERSPECTIVES ON MANET

Surendran et al. [5] proposed a QoS obliged inadequacy tolerant bug look-ahead guiding computation which tries to perceive real path and look-ahead path which may help in picking the substitute path if there ought to be an event of considerable route disillusionment.

The outcomes demonstrate that their calculation takes better directing choices with 20-30 percent improvement.

U. Verma et al. [6] introduce a powerful and secure system for confirmation of nodes in the MANET. They proposed validation protocol depends on testament trade between the nodes. Their protocol likewise utilizes computerized signature with a debris function to keep up the credibility of authentications. Reenactment showcase that this protocol shows better execution as far as throughput, start to finish postponement and bundle dropping in nearness of malicious nodes in the MANET. Moreover, it likewise had less calculation and correspondence overhead, which makes it reasonable for MANETs.

A. Jain et al. [7] state MANETs as a gathering of system gadgets which are associated through the wireless connections. It is utilized to trade the information. Thus, so as to make the correspondence in MANETs increasingly secure, they investigated a methodology dependent on trust technique to verify MANETs against attacks, for example, black hole attack, dim opening and DOS attack. Their proposed methodology distinguishes malignant node by processing trust estimation of the node. The methodology utilizes age of sham packets by the source node and sends to the goal node. Issue was taken as, to build up a methodology that can verify and improve the presentation of Reactive Routing Protocol family.

W. Mapenduka [8] depicts strategies which should work through the entire protocol stack since attacks target explicit layers. They talk about MANET attacks identification strategies that are presently being used observing their presentation. They additionally recommend a half and half cross-layer approach fit for identifying more than one known and new attacks, which can be investigated on to supplement existing strategies in building successful security answers for MANET.

H. Simaremare et al. [9] improves the introduction of Trust AODV using underground creepy crawly computation. Their convention is called Trust AODV Ant. The execution of creepy crawly computation in their protected convention is by adding an underground bug authority to put the positive pheromone in the node if the node is trusted. Underground creepy crawly master is addressed as a coordinating group. The pheromone worth is saved in the directing table of the node. They balanced the primary routing table by including the pheromone worth field. The manner in which correspondence was picked reliant on the pheromone obsession and the most constrained way. Trust AODV+ Ant is differentiated and fundamental straightforward insect routing calculation, AODV, and Trust AODV under DOS/DDOS attacks similar to execution. Re-establishment results show that the package movement extent and throughput of the Trust AODV increase in the wake of using underground creepy crawly count. In any case, similar to from beginning to end delay, there is no imperative improvement.

M. Gargan et al. [10] proposed a fluffy standard based methodology for plan and examination of a Trust-Based Secure Routing Protocol for MANETs (TBSRPM). Because of exceptionally powerful conduct of nodes the briefest course doesn't really ensure a protected course. Thus security of course isn't thought about as the course can be effectively break in the dynamic MANETs. Hence finding a steady and believed course is vital. Their calculation is the augmentation of the AODV, produced for making secure course between sources to goal. The protocol conduct relies upon TV and LOT just as TV chooses what level of security activity was required. So dependent on TV, the information bundle is encoded. With the assistance of TV, malicious nodes can be effectively wiped out and we can set up a best confided in course also. Results show that the TBSRP upgrades MANETs.

N. Saxena and J. Yi [11] proposed a power-mindful and completely non-interactive self-affirmation protocol dependent on bivariate polynomial mystery sharing and a non-interactive edge mark conspire. Conversely with earlier work, our methods don't require any cooperation and don't include any expensive solid communicate correspondence among MANET nodes. They completely examine our proposition and show that it looks at positively to past systems.

K. Govindanand P. Mohapatra [12] investigated the trust level of a node affects the certainty with which a substance conducts exchanges with that node. They present a point by point study on different trust figuring approaches that are equipped towards MANETs. Also, they break down different chips away at trust elements including trust spread, expectation and collection calculations, the impact of system elements on trust elements and the effect of trust on security networks.

R. Venkataraman et al. [13] proposed trust model was joined over AODV directing protocol and Optimized Link State Routing Protocol (OLSR) protocol in MANETs. The exhibition assessments show that via cautiously setting the trust parameters, considerable advantage as far as throughput can be gotten with negligible overheads. The registered trust and certainty esteems are brought into the way calculation procedure of the ad-hoc routing protocols. It was seen that the nodes in the system had the option to gain proficiency with the malevolent exercises of their neighbors and henceforth, substitute reliable ways are assumed to keep away from information misfortune in the system, with exchange offs in start to finish bundle postponement and routing traffic.

Table – I: Comparison of Different Trust Prediction Approaches.

Context in Use	Trust and Performance Metric	Advantages	Complexity	Performance and Limitation
Uses Kalman filter theory to predict the future trust values.	Trust is measured in [0], Prediction accuracy for various noise covariance matrix is analyzed [1].	Well established Kalman filter is used for prediction. The Prediction accuracy is higher.	Additional hardware complexity in implementing the feedback loop in Kalman filters.	This algorithm can be readily implemented with the expense of additional complexity as Kalman filter is a widely used prediction model.

Z. Yan and M. Wang [14] assists individuals with conquering impression of vulnerability and hazard and takes part in confided in social practices. They use two components of trust levels assessed by either a confided in server or individual PSN nodes or both to control PSN information access in a heterogeneous way based on property-based encryption. They officially demonstrate the security of our plan and break down its correspondence and calculation unpredictability. Broad examination and execution assessment dependent on usage show that their proposed plan was exceptionally effective and provably secure under pertinent framework and security models.

VIII. REVIEWS ON TRUST AND NOTORIETY BASED ROUTING PROTOCOLS

H. Yi [15] proposed authentication shows are restrictively costly and require critical correspondence among MANET focus focuses. They base on a normal sort of MANET that is kept on a brief explanation, and present a guaranteed, gainful, and an absolutely noninteractive confirmation technique planned for this kind of a system. Their confirmation show depends upon perplex sharing procedures utilizing bivariate polynomials. They in addition present another course of action that enables any pair of MANET focuses to beneficially set up an on-the-fly secure correspondence channel.

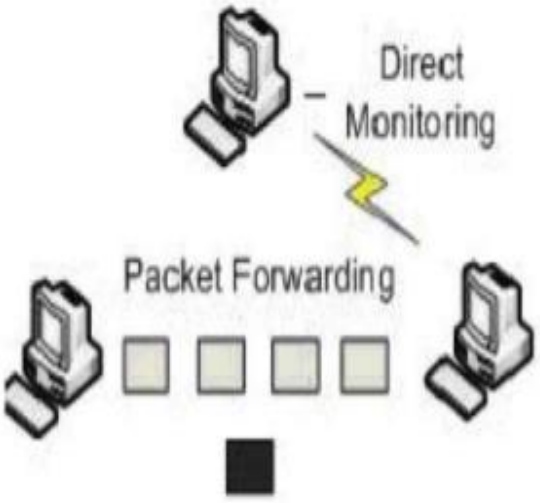

Fig.4. Direct Trust Observation

S. Joshi [16] secured all parts of trust the board and trust foundation crosswise over portable systems. The combination of secure multi-party calculation can give progressive ramifications towards trust discoveries and its pertinence inside MANET. The SMC protocols inferred different key realities as far as security protection while working with various imparting gatherings and protection conservation is one of the ideal worries in trust dissemination inside portable systems so this combination is the matter of worries of our work.

Rutvij H. Jhaveri et al. [17] performed affectability examination of TRS-PD which is finished by moving characteristics of different parameters specifically framework circumstances within the sight of three unquestionable group dropping attacks. Besides, their work gathers the attack structure disclosure framework, trust model, and routing segment grasped by TRS-PD in order to counter the adversaries which seek after certain attack plans close by various enemies. Assessments drove with organize test framework 2 show the correct choices of parameter regards for obvious framework circumstances.

Table- II: Influence of Different Trust Aggregation Approaches

Context in Use	Trust and Performance Metric	Advantages	Complexity	Performance and Limitation
Subjective logic-based trust aggregation.	Trust is represented as triplet in belief space. Set of theorems have been provided to prove various properties.	Trust is aggregated along with uncertainty. Hence the aggregated value is more reliable.	Additional hardware to implement the transformation between trust and belief spaces.	In the belief space every recommendation is given equal weight. Hence it is prone to attacks.

Aggregation of trust values using iterated belief and trust revision.	Trust is represented in [0] and [1]. Aggregation and operations are illustrated with examples.	The feedback revision of trust using max and median criterion is a effective method.	Complexity associated with belief and trust revision.	This aggregation can be used well in the belief-based trust system. The only limitation is associated complexity.
Weighted average combining of different trust values.	Trust is represented in [0] and [1]. Set of propositions have been provided to explain the various properties of aggregation operators.	The trust accumulated from different paths is given different weights and hence the chances for attacks are less.	Additional hardware to implement the push-sum and weighted averaging operations.	Less communication load as the gossips are aggregated into single value before retransmission.
Sequence and parallel aggregation operators are proposed.	Subjective logic is used to represent trust. Various aggregation operators are illustrated with examples.	Along with the trust certainty is also aggregated. This can increase the confidence on the aggregation result.	Additional hardware in terms of multiplications and weighted average.	This work proves the trust propagation through the shortest path may not be highly certain.

R. Cai et al. [18] proposed evolutionary self-cooperative trust (ESCT) plot that imitates human dynamic technique and depends upon trust-level data to anticipate particular coordinating disrupting impact ambushes. In their game plan, adaptable focuses will trade trust data and analyze got trust data dependent all alone enthusiastic judgment. Over the long haul, each node continuously propels its perception to disallow malicious components. The most appealing component of ESCT is that they can't deal the system paying little heed to whether the inside aggressors know how the security instrument capacities. They assess the presentation of ESCT plot under different routing interruption attack circumstances. Their results confirm that ESCT plan advances organize versatility and guarantees the directing viability within the sight of routing interruption aggressors in MANETs.

M. Gregory et al. [19] present MANET nodes transmit, hand-off and get traffic from neighbor nodes as the system topology changes. Security is significant for MANET and trust calculation is utilized to improve joint effort between nodes. MANET trust structures use ongoing trust calculations to keep up the trust state for nodes in the system. In the event that the trust calculation isn't strong against attack, the trust esteems registered could be questionable. They proposed an Artificial Immune System based way to deal with register trust and along these lines give a strong notoriety instrument.

K Dhanya [20] proposes an assessment on Trust Based Routing protocols to ensure Internet of Things coordinating to approve reliability and security in the midst of bearing discovering strategy in out of reach frameworks. There are different ways to deal with register trust for a node, for example, fluffy trust approach, trust organization approach, crossover approach, and so forth. They bring out quick of these methodologies for building up trust of the sharing center points in a dynamic and mysterious MANET atmosphere.

M. Riaz et al. [21] proposed trust model assesses trust by utilizing two fundamental segments: the immediate connection trust (Primary trust) determined utilizing the Bayesian measurable strategy and suggestions from the neighbors (auxiliary trust). The measurements utilized for ascertaining the essential trust are: the gotten sign quality, time of every cooperation, the closeness of nodes and the recurrence of connections. This trust surmising model is actualized over the traditional Dynamic Source Routing (DSR) protocol. The after effects of the recreations affirms, that the proposed model improve adequacy of routing in presence of malevolent friends in the MANETs.

Table – III: State of the existing work

Sr. No.	Author	Type of Security Attack	Proposition	Parameters Evaluated	Future Scope
1	M. Yu et al. [25]	Byzantine attack	develops a secure routing protocol called secure routing against collusion (SRAC) to defend Byzantine attacks as well as other internal attacks against routing protocols in adversarial environments	Throughput and Routing overhead was calculated taking seconds as reference frame. The average throughput evaluated was 15000 packets per second.	Working towards reducing the computational burden at each node during deployment of the network

2	M. Mohanapriya et al. [24]	Selective Blackhole attack	Presented a non-cryptographic and energy efficient protocol named as Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack where the destination node on detecting the malicious nodes (with the help of IDS), isolates them from the network. Also, IDS nodes will turn into random listening only in the presence of attack which results in less energy loss. Also, the packet loss rate came to be 64% lesser than DSR (Dynamic Source Routing)	Packet Drop Ratio, Control Packet Overhead and End-to-End Delay for MDSR and DSR protocols were evaluated in terms of node mobility and compared	To further reduce the percentage of packet loss and make the network more energy efficient
3	M. Ponguwala et al. [25]	Black hole and gray hole attacks in MANETs-IoT (Internet of Things)	Proposed Secure Group based Routing and Flawless Trust Formulation using Unsupervised Machine Learning Approach. Majority of attackers are identified by analyzing trust value.	evaluate the proposed work based on packet delivery ratio (PDR) and throughput.	To improve further energy efficiency of the adhoc network without loss in security.
4	J. Manoranjini et al. [26]	Black hole avoidance	Proposed a new trust model and analyzed the effectiveness of how a secured node can be routed inside the network. This trust model makes use of direct, indirect and mutual trust values between the sensor nodes.	Missed Detection Rate (MDR) and False Alarm Rate (FAR)were evaluated with respect to time	To further improve the performance of the network

IX. RESULTS

This paper analyses research articles based on the evaluated parameter which are generally termed as Quality of Service (QoS) [23]. In most of the cases, the following QoS parameters were observed.

a) $$Throughput = \frac{Total_{Receied_{Packets}}}{Total_{Simulation_{Time}}}$$ (1). [23]

b) $$PDR = \frac{number\ of\ packets\ transmitted\ by\ source\ node}{number\ of\ packets\ received\ by\ destination\ node}$$ (2). [25]

c) $$Packet\ Drop\ Ratio = \frac{number\ of\ packets\ not\ received}{total\ number\ of\ packets\ sent}$$ (3). [24]

d) $$MDR=\frac{Nmis}{N}\ and\ FAR=\frac{Nf}{Ni}$$ (4)

where N_f is the number of false packets, which is recognized as true packets, N_i is the total number of packets and N_{mis} is the number of true packets, which is recognized as false packets and N is the number of true packets.

X. CONCLUSION

All through the paper we tended to discuss every single part of the MANET and also about the security. Beginning from the scratch; we talked about the design of MANET, vulnerabilities of the MANET, diverse security dangers and even various sorts of security attacks in this paper. Non-stable design of MANETs and wireless vulnerabilities helped us to comprehend, why the MANETs are anything but difficult to attack. Layer shrewd system attacks and their proposed arrangements illuminated us to comprehend the method for activity and execution plan of various system attacks. From the entire scene one thing is perfectly clear that MANETs will go in transit in a similar manner with no significant change. Wireless is their characteristic partner as a correspondence medium; there is no substitution or option of wireless medium. These things will continue at any rate in not so distant future except if the rise of any new innovation. Despite the fact that there is the development on any substitution, it will take long to change to that specific innovation. At present we need to acknowledge the MANETs and wireless vulnerabilities as a decent shrewd. We can try to improve the things by remembering these vulnerabilities. For a minute on the off chance that we think decidedly, in reality we are honored with an incredible room, from inquire about perspective because of these vulnerabilities of the MANET and wireless medium. A great deal of research work has been finished by the scientists yet at the same time there is a ton to do. System security is a unique issue. New and new attacks are getting presented. So the steady endeavors are required to make the MANET increasingly secure. There is a great deal of research scope in the field of secure steering. Interruption location and its recuperating is another exploration problem area for the system security analysts. The majority of the interruption location frameworks and systems look lovely and persuading on papers yet at the same time applied

research work is hanging tight for the analysts in specific regions of system security. There is have to actualize, assess and improve these interruption location frameworks for all intents and purposes.

REFERENCES

1. Priyadsrini, "An Efficient Route Discovery in Manets with Improved Route Lifetime," Int. J. Inf. Electron. Eng., vol. 2, no. 4, pp. 2–5, 2012.
2. S. Sarika, A. Pravin, A. Vijayakumar, and K. Selvamani, "Security Issues in Mobile Ad Hoc Networks," Procedia - Procedia Comput. Sci., vol. 92, pp. 329–335, 2016.
3. A. Shabbir, F. Khalid, S. M. Shaheed, J. Abbas, and M. Zia-Ul-Haq, "Security: A Core Issue in Mobile Ad hoc Networks," J. Comput. Commun., vol. 03, no. 12, pp. 41–66, 2015.
4. P. K. Sharma and V. Sharma, "Survey on security issues in MANET: Wormhole detection and prevention," in Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016, 2017, pp. 637–640.
5. S. Surendran and S. Prakash, "An ACO look-Ahead approach to QOS enabled fault-tolerant routing in MANETs," China Commun., vol. 12, no. 8, pp. 93–110, 2015.
6. U. K. Verma, S. Kumar, and D. Sinha, "A secure and efficient certificate-based authentication protocol for MANET," in Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2016, 2016, pp. 1–7.
7. A. K. Jain and A. Choorasiya, "Protocol in Mobile Ad Hoc Network," no. Icces, pp. 958–964, 2017.
8. W. Mapenduka, "Methods for detecting attacks in mobile/wireless Ad-hoc networks: A survey," Int. J. Sci. Technol. Res., vol. 7, no. 7, pp. 168–174, 2018.
9. O. León, J. Hernández-Serrano, and M. Soriano, "Securing cognitive radio networks," Int. J. Commun. Syst., vol. 23, no. 5, pp. 633–652, 2010.
10. M. K. Garg, N. Singh, and P. Verma, "Fuzzy rule-based approach for design and analysis of a Trust-based Secure Routing Protocol for MANETs," in Procedia Computer Science, 2018, vol. 132, pp. 653–658.
11. N. Saxena and J. H. Yi, "Noninteractive Self-Certification for Long-Lived Mobile Ad Hoc Networks," vol. 4, no. 4, pp. 946–955, 2009.
12. K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," IEEE Communications Surveys and Tutorials, vol. 14, no. 2. IEEE, pp. 279–298, 2012.
13. R. Venkataraman, M. Pushpalatha, and T. Rama Rao, "Regression-based trust model for mobile ad hoc networks," IET Inf. Secur., vol. 6, no. 3, pp. 131–140, 2012.
14. Z. Yan and M. Wang, "Protect Pervasive Social Networking Based on Two-Dimensional Trust Levels," IEEE Syst. J., vol. 11, no. 1, pp. 207–218, 2017.
15. N. Saxena, G. Tsudik, and J. H. Yi, "Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 2, pp. 158–170, 2009.
16. S. Joshi and D. K. Mishra, "A roadmap towards trust management & privacy preservation in mobile ad hoc networks," in Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016, 2017, pp. 1–6.
17. R. H. Jhaveri, N. M. Patel, Y. Zhong, and A. K. Sangaiah, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT," IEEE Access, vol. 6, pp. 20085–20103, 2018.
18. R. J. Cai, X. J. Li, and P. H. J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," IEEE Trans. Mob. Comput., vol. 18, no. 1, pp. 42–55, 2019.
19. L. E. Jim and M. A. Gregory, "AIS Reputation Mechanism in MANET," in 2018 28th International Telecommunication Networks and Applications Conference, ITNAC 2018, 2019, pp. 1–6.
20. K. Dhanya, C. Jeyalakshmi, and A. Balakumar, "A Secure Autonomic Mobile Ad-hoc Network based Trusted Routing Proposal," in 2019 International Conference on Computer Communication and Informatics, ICCCI 2019, 2019, pp. 1–6.
21. M. K. Riaz, F. Yangyu, and I. Akhtar, "A multidimensional trust inference model for the mobile Ad-Hoc networks," in 2019 28th Wireless and Optical Communications Conference, WOCC 2019 - Proceedings, 2019, no. Wocc, pp. 1–5.
22. A. Kumar et al., "Destination based group Gray hole attack detection through MANET in AODV", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012.
23. M. Yu et al., "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions on vehicular technology 58(1), 449-460, 2008
24. M. Mohanapriya et al., "Modified DSR protocol for detection and removal of selective black hole attack in MANET.", in Computer & Electrical Engineering 40(2), 530-538, 2014.
25. M.Ponguwala et al., "Secure Group based Routing and Flawless Trust Formulation in MANET using Unsupervised Machine Learning Approach for IoT Applications", EAI Endorsed Transactions on Energy Web 6(24), 2019.
26. J. Manoranjini et al., "Improved QoS and avoidance of black hole attacks in MANET using trust detection framework", Automatika 1-11, 2019.

AUTHORS PROFILE

Ravneet Kaur Sidhu*, Research scholar, Department of Computer Science, Punjabi University, Patiala, India **Email: ravneetsidhu21@ymail.com**

Ram Krishan, Assistant Professor, Department of Computer Science, Guru Kashi Collage, Punjabi University, Talwandi Sabo, India **Email: ramkrishan@pbi.ac.in**