I.J. Wireless and Microwave Technologies, **2020, 1, 38-47**
Published Online February 2020 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2020.01.04

Available online at ***http://www.mecs-press.net/ijwmt***

A Comprehensive Mechanism of MANET Network Layer Based Security Attack Prevention

[1]Mahaboob Sharief Shaik, [2]Fahad Mira

[1]Research Scholar, JJT university,Rajasthan India.
[2]Assistant Professor, Jeddah International College, Jeddah, Kingdom of Saudi Arabia

Received: 02 October 2019; Accepted: 26 December 2019; Published: 08 February 2020

Abstract

The infrastructure benefits, which are achieved from the MANET architecture is the prime reason for the increase in usage for various purposes. The MANET architecture is made truly seamless with the capabilities of working without the central base stations or without the intervention of the central administration. The architecture for a MANET network is highly diversified and completely depends on the formation as the nodes in the MANET network can roam freely with a subsequent connection to any external device or any external networks. Yet another primary benefit of these devices and the networks are operability of the networks and the nodes without any human interventions. This property of the MANET network nodes makes the MANET devices operable in extreme conditions, where the human interventions are nearly impossible. In spite of these uncountable benefits, the MANET networks and the devices, which are part of the networkare always subjected to attacks from various sources. In this work, the attacks types for each network layer are identified and addressed to be prevented. The measures listed in this work are convertible as a modular component of any automated framework to make the complete attack prevention mechanism automated

Index Terms: MANET, MANET Layers, MANET Attacks, Attack Prevention, Selfishness, Rushing, Routing table overflow, BlackHole, Jamming

1. Introduction

The MANET routing protocols are the most targeted factor for the attacks. The consequences of the attacks are disastrous as the attacks can distort the routing table, network architectures, node placements, incorrect

* Corresponding author
E-mail address: smshariefkaau@gmail.com, f.mera@jicollege.edu.sa

routing and sometimes the malicious node incorporations, which can degrade the performance of the entire network.The work ofP. Mohapatra et al. [1] elaborates on the network protocols and the attack types. Various parallel research attempts have classified the attacks on the MANET network in primarily two categories based on data shared in the network as Active and Passive Attacks. The work by N. Milanovic et al. [2] and A. F. Farhan et al. [3] have clearly classified the differences between these two types of attacks. In PC organizing, a parcel drop assault or blackhole assault is a sort of forswearing of-administration assault in which a switch that should hand-off bundles rather disposes of them. This typically happens from a switch getting to be undermined from various causes. One reason referenced in research is through a refusal of-administration assault on the switch utilizing a known DDoS instrument as demonstrated by J.-H. Cho et al. [4].

An aloof assault on a cryptosystem is one in which the cryptanalyst can't collaborate with any of the gatherings included, endeavouring to break the framework exclusively dependent on watched information (for example the ciphertext). This can likewise incorporate known plaintext assaults where both the plaintext and its comparing ciphertext are known as explored by B. Wu et al. [5].

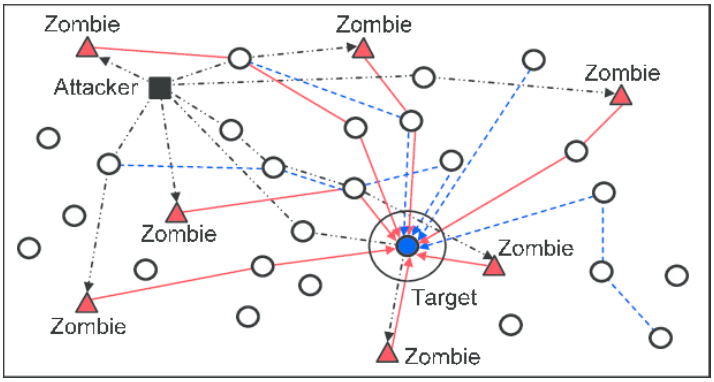


Fig. 1. Internal and External Attack Classification Based on Node Location

During the internal attacks, the complete network is under threat as the attacking node cannot be isolated and the complete network can fall apart. The work by Y. Xiao et al. [6] in the year of 2007 and the work by K. A. Farhan et al. [7] in the year 2008 have clearly listed the damages can be caused by the internal attacks.

In the other hand, the external attacks completely rely on the trust management mechanism of the network. Trust foundation and the executives in MANETs face difficulties because of asset imperatives and the mind-boggling interdependence of systems. Overseeing trust in a MANET needs to consider the connections between the composite psychological, social, data and correspondence systems, and consider the asset limitations, and elements.The significant proofs are listed by H. M. Deng et al. [8] and also by A. Mishra et al. [9] to support this discussion.

Regardless to mention, that the network attacks are occurring on various layers of the network and the prevention method should be built on the specific layers as a component for the complete framework.

With an occasion evolving system it's evident we have to expect variations in system operation as a result of no stationary structure (no stationary connections). Additional since media topology determines disturbance and so connectivity, the freedom pattern of apparatus within the system will affect system operation, potentially causing data being forced to be re sent plenty of that time period (increased delay) last but not least allocation of network tools like power remains cloudy.

2. Outcome of the Parallel Researches

In this area of the work, the parallel research results are investigated. This work tended to two associated research issues as conveyed inquiry preparing and assault recognition for appropriated group component, consequently the review of the ongoing examination results is additionally characterized into two sections.

The circulated question handling has consistently been reprimanded for higher time multifaceted nature. The main Endeavor to lessen the time multifaceted nature was proposed by Jens Dittrich et al. [10]. The result of that exploration was persuading. In any case, the improvement of that work was proposed by Jorge-Arnulfo et al. [11] for making a nonexclusive prescient system to foresee the better performing hubs and inquiries running on those hubs or bunches.

During the handling of the questions on grouped design, the distinguishing proof of the information and traits utilized in the inquiries are the most basic segment of the examination. The work by Mohamed Y. Eltabakh et al. [12] have shown a novel methodology for information disclosure. During the information disclosure stage, aggregating the traits utilized in the inquiry is one of the prime elements. Consequently, the work by Yuting Lin et al. [13] pulled in a great deal of considerations from the analyst's locale.

One more test of the current research is to be manufacture the subjective information and dole out the information to the fitting undertakings on the circulated systems. The designation of the information to the undertakings can be overseen by any of the Map-Reduce system, by the by, the structure of informational collections must be taken care of independently. To take care of this issue, Songting Chen et al. [14] introduced a novel result of the exploration.

Along these lines, the assault identification on the conveyed information is exceptionally mind boggling and many the assault occasions just creates the negative psychological effects because of the assaults. The work by Y. Liang et al. [15] have shown a contextual analysis to understand the impact and headings of the assaults via web-based networking media information.

One of the real assault types have shown that creation strategy related data accessible to the online networking can likewise be considered as assault. Crafted by W. Chung et al. [16]. The further and more profound assaults on the social information can be producing impact dependent on the psychological information and crafted by I. Outrage et al. [17] have exhibited a novel way to deal with recognize such sorts of assaults.

In the next section of the work, based on the parallel research outcomes, the vulnerable areas of the MANET networks and the attack types are discussed.

3. Vulnerability and the Attack Types

In this section of the work, the most vulnerable segments of the MANET architectures are discussed. Subsequently, the types of the attacks are also discussed. The outcome of this section of the work shall make the design of the proposed algorithm, which is presented in the next section more specific and efficient in nature.

A. Vulnerable Components of the MANET network

Firstly, the vulnerable sections of the MANET networks are discussed here:

- **Dynamically Changing Network Topology**: The undeniable intrigue of MANETs is that the system is decentralized, and hubs/gadgets are portable, in other words there is no fixed foundation which gives the likelihood to various applications in various territories, for example, natural checking catastrophe help and military correspondences. Since the mid-2000s enthusiasm for MANETs has incredibly expanded which, to a limited extent, is because of the reality versatility can improve arrange limit.

- **Transmission Links**: Since system topology decides impedance and along these lines availability, the portability example of gadgets inside the system will effect on system execution, perhaps bringing about information being despise a ton of times as expanded deferral lastly allotment of system assets, for example, control stays vague. At last, finding a model that precisely speaks to human portability while remaining numerically tractable remains an open issue because of the enormous scope of elements that impact it. Some regular models utilized incorporate the irregular walk, arbitrary waypoint and duty flight models.
- **Decentralized Management**: The MANET networks are prone to attacks due to the lack of centralized monitoring of the complete network. Thus, the node under attack can also be the management node of cluster head node.

B. Attack Type Analysis

Secondly, due to the posted compromising factors in the architecture, the following attacks can be observed in the MANET networks:

- **Interrogation Attack*:*** This attack repeatedly sends RTS messages to any selective node in order to drain the resources and received the CTS responses.
- **Energy Drain Attack:** This attack introduces high amount of network traffic in order to drain the energy of any network and as a result the number of dead nodes increases in the network. The types of drain attacks are surveyed by Dubey et al. [18] and presented in comparative framework.
- **Hello Flood Attack*:*** This attack sends huge pile of "Hello" packets in the network by broadcasting and as a result the life time of the network reduces significantly. The types of flood attacks are surveyed by Singh et al. [19] and presented in comparative framework.
- **Misdirection Attack*:*** The main objective of the intruder is to misdirect the incoming messages to increase the latency, which prevents a few packets from reaching the base station. It is been observed by the work of Abdullah et al. [20] that this attack can be identified by the nodes receiving data packets out of the regular pattern.
- **Flooding Attack*:*** The main purpose of this attack is to deliberately communicate to a single node in order exhaust the resource limit or the connection limit. Yet another contribution by Dubey et al. [21] has demonstrated the classifications and implications.
- **Jamming Attack*:*** This attacks cause denies of connection or access requests by the authorised clients of the network. The types of the jamming attacks are classified by Pelechrinis et al. [22] as an outcome of his popular survey.
- **Collision Attack*:*** The collision attacks are introduced by sending a data packet with noises in order to disrupt the actual transmission. The collision attacks are extensively studied and presented by Reindl et al. [23].
- **Black Hole Attack*:*** The black hole attacks cause a high packet loss in the network. This attack types alter the routing protocols in order to divert all packets to a specific node and then discard the packets. The black hole attacks are been deeply examined and presented by Ramaswamy et al. [24].
- **Denial of Service Attack*:*** The widely encounter attacks are the DoS attacks and this attack type can damage any resource of the network. The varieties of this attack type were thoroughly studied and presented by J. Ding et al. [25].
- **Selective Forwarding Attack*:*** The selective forwarding attack can often be confusing with the firewall protocols as certain nodes refuses to forward few packets in the network causing interruption in the service or the broadcasts. This phenomenon was elaborated by Y. Zhang et al. [26].

These mentioned attacks can significantly destroy the MANET architecture. The parallel research outcomes discussing the damage severities are listed here. Aly M. El-Semary et al. [27] mentioned that A grouping approach in AODV steering convention for the identification and avoidance of dark gap assault in MANETs has been proposed. The other parallel research outcome by B. Muneeswari et al. [28] have showcased that MANETS can be utilized for encouraging the accumulation of sensor information for information digging for an assortment of uses, for example, air contamination observing and various kinds of models can be utilized for such applications. A key normal for such applications is that adjacent sensor hubs observing a natural element ordinarily register comparative qualities. This sort of information repetition because of the spatial connection between sensor perceptions rouses the strategies for in-organize information accumulation and mining.

The recent research by Jin-Hee Cho et al. [29] have significantly identified that to portray the necessities of an application, it very well may be classified as either steady checking, occasion observing, consistent mapping or occasion mapping. Steady sort applications are time sensitive and all things considered information is produced occasionally, while occasion type applications are occasion drive thus information is possibly created when an occasion happens. The observing applications are always running over some undefined time frame, though mapping applications are generally conveyed once so as to survey the present condition of a wonder. The similar concept was defended by Jia Liu et al. [30] and Jiankang Zhang et al. [31].

Henceforth, as outcome of the literature survey, this work presents the impact of each popular attack on the network parameters in order to build the proposed framework with the recommendation system [Table. 1].

Table 1. Types of Attacks with Influence on Network Node Characteristics

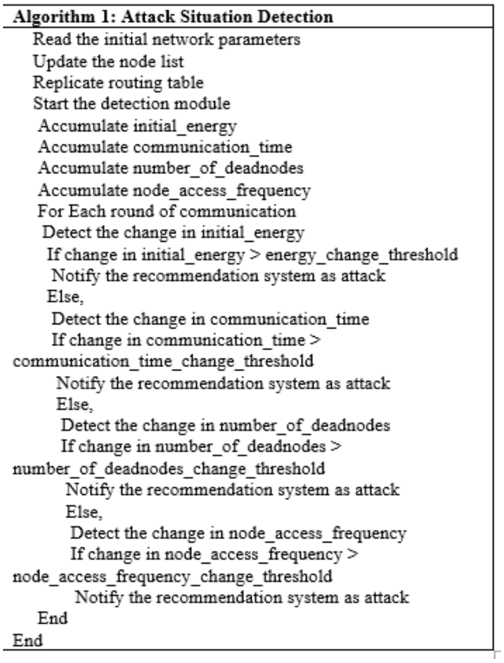
Attack Type	**Energy**	**Delay**	**Routing Pattern**	**High Traffic**	**Dead Node**
Interrogation	Yes	No	No	Yes	No
Energy Drain	Yes	No	No	Yes	Yes
Hello Flood	Yes	No	No	No	Yes
Misdirection	No	No	Yes	Yes	No
Flooding	Yes	Yes	No	Yes	Yes
Jamming	No	No	Yes	No	No
Collision	No	Yes	No	No	No
Black Hole	No	No	Yes	No	No
Denial of Service	No	No	Yes	No	No
Selective Forwarding	No	No	Yes	No	No

Thus, this measure will certainly help in order to model the attacks during simulation and build the proposed framework.

4. Proposed Algorithm

In this section of the work, the algorithm for detecting the attack situations is furnished.

The malicious router may also reach this strike, e.g. by dropping packets for a specific system destination, either at a specific period of the evening, a package every n packs or each t minutes, or even perhaps a randomly selected percentage of those packs. That really is pretty referred to as a greyhound attack. In the event the malicious router tries to lose all packets which arrive from, the strike can be discovered fairly fast through shared networking tools like traceroute. Additionally, when other routers discover the endangered router is falling traffic, they'll normally start to get rid of that router out of their forwarding tables and no traffic will flow into the strike. But in the event the malicious router begins dropping packets to a particular period of time or higher every n packs, then it's harder to find because some traffic flows throughout the system.



Algorithm 1: Attack Situation Detection

```
    Read the initial network parameters
    Update the node list
    Replicate routing table
    Start the detection module
     Accumulate initial_energy
     Accumulate communication_time
     Accumulate number_of_deadnodes
     Accumulate node_access_frequency
     For Each round of communication
      Detect the change in initial_energy
       If change in initial_energy > energy_change_threshold
        Notify the recommendation system as attack
       Else,
        Detect the change in communication_time
        If change in communication_time >
communication_time_change_threshold
         Notify the recommendation system as attack
         Else,
          Detect the change in number_of_deadnodes
          If change in number_of_deadnodes >
number_of_deadnodes_change_threshold
           Notify the recommendation system as attack
           Else,
            Detect the change in node_access_frequency
            If change in node_access_frequency >
node_access_frequency_change_threshold
             Notify the recommendation system as attack
     End
End
```

Based on the recommendation generated from this algorithm, the recommendation system will suggest the counter measures for the attacks.

5. Results and Discussions

In this section of the work, the work presents and discusses the results.

The first simulation of the attack on the proposed framework was on the simulated network attack. The observations on the network parameters are furnished here [Table. 2].

Table 2. Network Parameter Observation on Energy Drain Attack

1	2 (Sec)	3 (Sec)	4	5	6 (Joule)	7 (Joule)
Round - 1	0.09	0.01	0	0	0.099481	0.089502
Round - 2	0.022	0.024	0	0	0.098941	0.078898
Round - 3	0.012	0.016	0	0	0.09838	0.068379
Round - 4	0.01	0.01	0	0	0.097773	0.057797
Round - 5	0.018	0.014	0	0	0.097191	0.047193
Round - 6	0.008	0.008	0	0	0.096651	0.036653
Round - 7	0.01	0.01	0	0	0.09607	0.026071
Round - 8	0.01	0.01	0	0	0.095531	0.015489
Round - 9	0.01	0.008	0	0	0.094969	0.0049281
Round - 10	0.012	0	0	20	0.094384	0

1. Rounds, 2. CommunicationTime (without Any Attack), 3. CommunicationTime (with Attack), 4. DeadNodes (without Any Attack), 5. DeadNodes (with Attack), 6. AverageEnergy (without Any Attack), 7. AverageEnergy (with Attack)

It is to be observed here that there is a drastic drop in the node energy levels. However, the communication time remains same. Hence it is natural to understand that there is no significant change in the data load on the network. But the drastic drop in the energy level denotes an attack on the network which is causing the energy drains.

The results are compared visually here [Fig. 2 and Fig. 3].

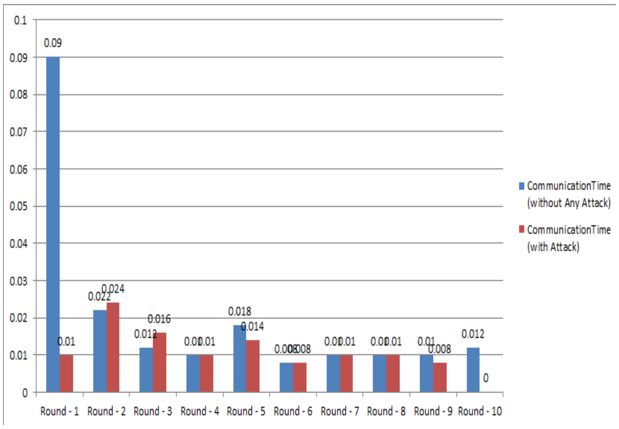


Fig. 2. Communication Time

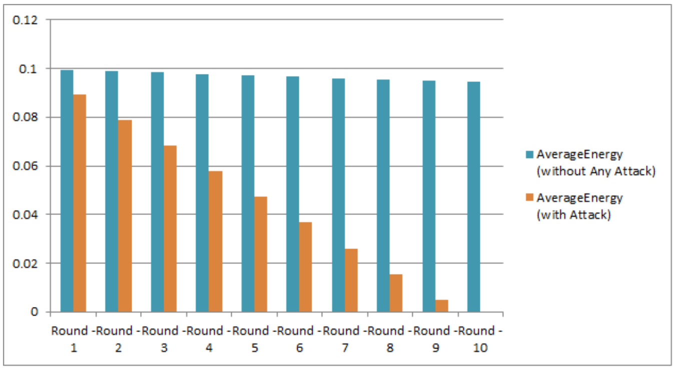


Fig. 3. Energy Reduction

6. Conclusion

The universe of remote correspondence is addition on board the game plan enthusiasm for remote sensors. the need to technique information to boot demands the motivation of remote detecting component frameworks. The plan for a painter system is exceptionally wide-running and completely relies upon the development in light of the fact that the hubs inside the painter system will float unreservedly with a later relationship to any outside gadget or any outer systems. Eventually, the needs for the assurance for these sent frameworks can't be unnoticed. to oversee satisfactory security instrument is that the might want of the recurring pattern analyse. The package drop attack might be usually set up to strike wireless adhoc networks. As wireless networks possess a far different design than that of an average wired system, a server may broadcast it has got the shortest path towards a destination. As a result, all traffic will be made to the server that's been compromised, and also the server can shed packets twill. In this manner, this work examinations the kinds of attacks on WSN and gives a conventional structure to separate the strikes dependent on the framework parameters. for sure, the nonattendance of ambush check frameworks intrigued this work to produce partner through and through pushed attack check framework structures to take a gander at the progressions inside the framework parameters. This outcome can sure as shooting encourage in structure a great deal of framework styles with high security. The work to boot adds to the counter measures all through any strike, during this way manufacturing a predominant world for remote detecting component frameworks.

References

[1] P. Mohapatra, S. Krishnamurthy, AD HOC NETWORKS: Technologiesand Protocols. Secaucus, NJ, USA:Springer-Verlag New York, Inc, 2004.

[2] N. Milanovic, M. Malek, A. Davidson, V. Milutinovic, "Routing and security in mobile ad hoc networks", Computer, vol. 37, pp. 61-65, February 2004.

[3] A. F. Farhan, D. Zulkhairi, M. T. Hatim, "Mobile agent intrusion detection system for Mobile Ad Hoc Networks: A non-overlapping zone approach", 2008 4th IEEE/IFIP International Conference on Central Asia on Internet Tashkent, pp. 1-5, 2008.

[4] J.-H. Cho, I.-R. Chen, P.-G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks", Reliability IEEE Transactions on, vol. 59, no. 1, pp. 231-241, 2010.

[5] B. Wu, J. Chen, J. Wu, M. Cardei, Y. Xiao, X. S Shen, D.-Z Du, "A survey of attacks and countermeasures in mobile ad hoc networks" in Wireless Network Security, Springer US, pp. 103-135, 2007.

[6] Y. Xiao, X. Shen, D.-Z. Du, Wireless Network Security (Signals and Communication Technology), Secaucus, NJ, USA:Springer-Verlag New York, Inc, 2007.

[7] K. A. Farhan, "Network Sender Multicast Routing Protocol", Seventh International Conference on Networking (icn 2008), pp. 60-65, 2008.

[8] H. M. Deng, W. L, D. P Agrawal, "Routing security in wireless ad hoc networks", Communications Magazine IEEE, vol. 40, pp. 70-75, Oct. 2002.

[9] A. Mishra, K. Nadkarni, A. Patcha, "Intrusion detection in wireless ad hoc networks", Wireless Communications IEEE, vol. 11, pp. 48-60, Feb. 2004.

[10] Jens Dittrich, Jorge-Arnulfo Quiané-Ruiz, Alekh Jindal, YagizKargin, Vinay Setty, JörgSchad, Hadoop++: making a yellow elephant run like a cheetah

[11] Jens Dittrich, Jorge-Arnulfo Quiané-Ruiz, Stefan Richter, Stefan Schuh,Alekh Jindal, JörgSchad, Only aggressive elephants are fast elephants

[12] Mohamed Y. Eltabakh, Yuanyuan Tian, FatmaÖzcan, Rainer Gemulla, AljoschaKrettek, John McPherson, CoHadoop: flexible data placement and its exploitation in Hadoop, Proceedings of the VLDB Endowment, v.4 n.9, p.575-585, June 2011 [doi>10.14778/2002938.2002943]

[13] Yuting Lin, Divyakant Agrawal, Chun Chen, Beng Chin Ooi, Sai Wu, Llama: leveraging columnar storage for scalable join processing in the MapReduce framework, Proceedings of the 2011 ACM SIGMOD International Conference on Management of data, June 12-16, 2011, Athens, Greece [doi>10.1145/1989323.1989424]

[14] Songting Chen, Cheetah: a high performance, custom data warehouse on top of MapReduce, Proceedings of the VLDB Endowment, v.3 n.1-2, September 2010 [doi>10.14778/1920841.1921020]

[15] Y. Liang, X. Zheng, D. D. Zeng, X. Zhou, S. J. Leischow, W. Chung, "Exploring How the Tobacco Industry Presents and Promotes Itself in Social Media", Journal of Medical Internet Research, vol. 17, no. 1, 2015.

[16] W. Chung, D. Zeng, "Social-Media-Based Public Policy Informatics: Sentiment and Network Analyses of U.S. Immigration and Border Security", Jrnl. Asso. for Information Science and Technology, vol. 67, no. 7, pp. 1588-1606, 2016.

[17] I. Anger, C. Kittl, "Measuring Influence on Twitter", Proc. the 11th Intl. Conf. on Knowledge Management and Knowledge Technologies, 2011.

[18] Dubey, A.; Jain, V.; Kumar, A. A Survey in Energy Drain Attacks and Their Countermeasures in Wireless Sensor Networks. Int. J. Eng. Res. Technol. 2014, 3. Sensors , 16, 1932 27 of 27

[19] Singh, V.P.; Jain, S.; Singhai, J. Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. Int. J. Comput. Sci. Issues 2010, 7, 23–27.

[20] Abdullah, M.Y.; Hua, G.W.; Alsharabi, N.Wireless sensor networks misdirection attacker challenges and solutions. In Proceedings of the International Conference on Information and Automation, Changsha, China, 20–23 June 2008; pp. 369–373.

[21] Dubey, A.; Meena, D.; Gaur, S. A Survey in Hello Flood Attack in Wireless Sensor Networks. Int. J. Eng. Res. Technol. 2014, 3.

[22] Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of service attacks in wireless networks: The case of jammers. IEEE Commun. Surv. Tutor. 2011, 13, 245–257.

[23] Reindl, P.; Nygard, K.; Du, X. Defending malicious collision attacks in wireless sensor networks. In Proceedings of the IEEE/IFIP Conference on Embedded and Ubiquitous Computing (EUC), Hong Kong, China, 11–13 December 2010.

[24] Ramaswamy, S. Prevention of Cooperative Blackhole Attack in Wireless Ad-hoc Networks. Int. Conf. Wirel. Netw. 2003, 2003, 1–7.

[25] Ding, J. Defending against path-based DoS attacks in Wireless Sensor. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '05), New York, NY, USA, 7 November 2005; pp. 89–96.

[26] Zhang, Y.; Minier, M. Selective Forwarding Attacks against Data and ACK Flows in Network Coding and Countermeasures. J. Comput. Netw. Commun. 2012, 2012, 184783.

[27] Aly M. El-Semary ;HossamDiab, BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map, IEEE Access, 2019

[28] B. Muneeswari ; M.S.K. Manikandan, Energy efficient clustering and secure routing using reinforcement learning for three-dimensional mobile ad hoc networks, IET Communications, 2019

[29] Jin-HeeCho ; Hamid Al-Hamadi ; Ing-Ray Chen, COSTA: Composite Trust-Based Asset-Task Assignment in Mobile Ad Hoc Networks, IEEE Access, 2019

[30] JiaLiu ; Yang Xu ; Zhao Li, Resource Allocation for Performance Enhancement in Mobile Ad Hoc Networks, IEEE Access, 2019

[31] JiankangZhang ;Taihai Chen ; ShidaZhong ; Jingjing Wang ; Wenbo Zhang ; Xin Zuo ; Robert G. Maunder ; Lajos Hanzo, Aeronautical Ad Hoc Networking for the Internet-Above-the-Clouds, Proceedings of the IEEE, 2019.

Authors' Profiles

Mahaboob Sharief Shaik has completed master's degree in computer applications in the year 1998 and presently, is a research scholar at JJT University, worked as lecturer at faculty of computing & information technology, King abdulaziz university, Jeddah, Saudi Arabia. His area of interest is network/information security, image processing and database.

Dr.Fahad Mira has completed PhD in computer science, and presently working as faculty member in Jeddah International College, and his area of research IncludesNetwork/Information/Cybersecurity.

How to cite this paper: Mahaboob Sharief Shaik, Fahad Mira, " A Comprehensive Mechanism of MANET Network Layer Based Security Attack Prevention ", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.10, No.1, pp. 38-47, 2020.DOI: 10.5815/ijwmt.2020.01.04