ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

Network Layer Attacks Mechanisms in MANETS-A Survey

[1]Inam Ullah Khan,[2] Muhammad Abul Hassan
[1]Isra University School of Engineering and Applied Sciences (SEAS)
[2]Abdul Wali Khan University Mardan, KPK, Pakistan
Email address:[1]Inamullahkhan05@gmail.com, [2]abulhassan900@gmail.com

Abstract- The security issue in versatile adhoc networks is to shield the network layer from noxious assaults, subsequently recognizing and avoiding malevolent hubs. A brought together security is in particularly requirement for such networks to ensure both course and information sending operations in the network layer. The noxious hubs in the network can promptly act to work as switches. This will exclusively aggravate the network operation from right conveying of the bundles, similar to the vindictive hubs can give stale directing upgrades or drop every one of the parcels going through them. This paper also focuses on different security aspects of network layer and discusses the effects of the attacks in detail through a survey approaches used for security purposes.

Keywords-Mobile Ad hoc network, network- layer attacks, Security.

I. INTRODUCTION

Portable Ad Hoc Networks are framed by remote hosts which might be versatile. There is no previous infrastructure Routes between hubs may possibly contain various jumps. Versatile specially appointed system (MANET) is a self-designing framework less system of cell phones associated by remote. Specially appointed is Latin and signifies "for this reason". Every gadget in a MANET is allowed to move autonomously in any bearing, and will in this manner change its connections to different gadgets much of the time. Each must forward activity irrelevant to its own particular use, and in this manner be a switch [1-3]. The essential test in building a MANET is preparing every gadget to persistently keep up the data required to appropriately course activity. Such systems may work without anyone else or might be associated with the bigger Internet. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. The growth of laptops and 802.11/Wi-Fi wireless organizing have made MANETs a well known exploration subject following the mid-1990s. Numerous scholastic papers assess conventions and their capacities, expecting fluctuating degrees of versatility inside a limited space, for the most part with all hubs inside a couple jumps of each other. Distinctive conventions are then assessed in view of measure, for example, the bundle drop rate, the overhead presented by the directing convention, end-to-end parcel delays, system throughput and so on. Security is a key administration for remote system interchanges. Be that as it may, the qualities of MANETS stance both difficulties and opportunities in accomplishing security objectives, for example, confidentiality, Authentication, trustworthiness, accessibility, access control, and non-revocation [4]. The countermeasures can be considered as elements or capacities that diminish or kill security vulnerabilities and assaults [5-8]. To start with, in this paper a diagram of system layer assaults is given, and after that the security counter measures.

The hubs in MANET can convey straightforwardly in the event that they are in inside each other's remote transmission runs else they need to depend on some different hubs to transmit messages if the hubs are outside each other's transmission range [9-11]. Hence, a few middle of the road has hand-off the parcels which are sent by the source host before they achieve the destination host, which thus prompts a multi-jump situation I.e. every hub, will go about as a switch. The hubs collaboration is particularly essential for a fruitful correspondence. In this manner, a MANET has a few striking qualities dynamic topologies, asset constraints,limited physical security, and no base. Possibleapplications of MANET include: Soldiers transferring data forsituational mindfulness on the war zone, business partners.

Sharing information during a meeting; attendees using laptopcomputers to participate in an interactive

ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

conference; andemergency disaster relief personnel coordinating efforts after afire, hurricane, or earthquake. The other possible applicationsinclude personal area and home networking, location-basedservices, and sensor networks [11-24]. There are a wide variety of attacksthat target the weakness of MANETS. For example, routingmessages are an important component of mobile networkcommunications, as each packet needs to be passed quicklythrough intermediate nodes, which the packet must traverse froma source to the destination. Malicious routing attacks can targetthe routing discovery or maintenance phase by not following thespecifications of the routing protocols. There are also attacks thattarget some particular routing protocols, such as DSR, or AODV. More sophisticated and subtle routing attacks have beenIdentified in recent published papers, such as the black hole (orSinkhole), Byzantine, and wormhole attacks.

II. NETWORK SECURITY ATTACKS

The connectivity of mobile nodes over a wireless link in MANETS which is multi hop in nature strongly relies on the fact that ensures cooperation among the nodes in the network. Since network layer protocols forms connectivity from one hop neighbors to all other nodes in MANET, the assurance of cooperation among nodes is required. Recently variety of network layer targeted attacks have been identified and heavily studied in research papers [25-43]. As a result of assaulting system layer directing conventions, enemies can without much of a stretch irritate and retain system activity, infuse themselves into the chose information transmission way between the source and destination, and along these lines control the system movement stream, as appeared in Figure 1, where a malignant hub M can meddle itself in the middle of any of the transitional hubs partaking in the correspondence in the picked way (in the figure 1 to N speaks to the quantity of moderate hubs) between source S and destination D.

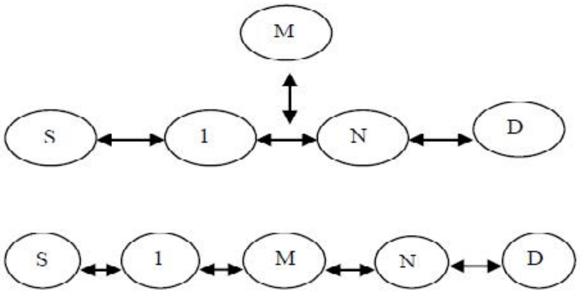
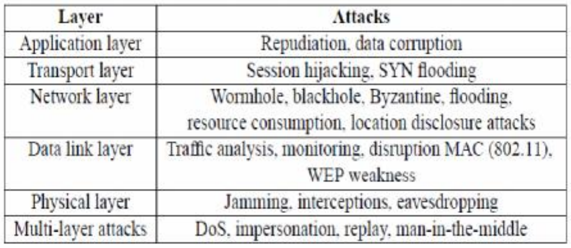


Figure 1: Interference of malicious node in between sourceand destination communication

The main effect of the presence of malicious nodes in the network is excessive network control traffic which intensifies the network congestion and as a result the performance of the network degrades.

a. Security Attacks

An assortment of assaults are conceivable in MANET. A few assaults apply to general system, some apply to remote system and some are particular to MANETs. These security assaults can be grouped by criteria, for example, the do-fundamental of the assailants, or the procedures utilized as a part of assaults.



Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

Figure 2: Attacks at Various Layers

These security attacks in MANET and all other networks can be roughly classified by the following criteria: passive or active, internal or external.

b. Passive vs. active attacks

The assaults in MANET can generally be arranged into two noteworthy classifications, to be specific aloof assaults and dynamic assaults. A latent assault acquires information traded in the system without upsetting the operation of the correspondences, while a dynamic assault includes data interference, alteration, or creation, along these lines disturbing the ordinary usefulness of a MANET. Table 1 demonstrates the general scientific classification of security assaults against MANET. Case of inactive assaults are spying, movement investigation, and activity checking. Case of dynamic assaults incorporate sticking, imitating, adjustment, foreswearing of administration (DoS), and message replay

.Internal vs. external attacks

The assaults can likewise be characterized into outside assaults and inner assaults, agreeing the area of the assaults. A few papers allude to outcast and insider assaults . Outer assaults are completed by hubs that don't have a place with the area of the system. Inner assaults are from traded off hubs, which are very of the system. Interior assaults are more serious when contrasted and outside assaults subsequent to the insider knows profitable and mystery data, and has special access rights.

Cryptography vs. non-cryptography related attacks

Some attacks arenon-cryptography related, and others are cryptographic primitive attacks.

Physical layer attacks

Wireless communication is broadcast by nature. A common radio signal is easyto jam or intercept. An attacker could overhear or disrupt the service of a wirelessnetwork physically.

Interference and Jamming

Radio signals can be jammed or interferedwith, which causes the message to be corrupted or lost. If the attackerhas a powerful transmitter, a signal can be generated that will be strongenough to overwhelm the targeted signals and disrupt communications. Themost common types of this form of signal jamming are random noise andpulse. Jamming equipment is readily available. In addition, jamming attackscan be mounted from a location remote to the target networks.

III. OPEN CHALLENGES AND FUTURE DIRECTIONS

Security in MANETS is such a hot topic among the research communities, if it is assured properly it can be used as a success factor and for the widespread deployment of the network. Several types of attacks in network layers have been identified and analyzed recently in most research papers. Security countermeasures and the defense against for each of the network attacks so far designed and implemented for MANETS are presented in the above sections. The research proposals till date, in MANETS are based upon a specific attack. They could work well in the presence of designated attacks, but there are many unanticipated or combined attacks that remain undiscovered. A lot of research is still on the way to identify new threats and create secure mechanisms to counter those threats. More research can be done on the robust key management network, trust-based protocols,integrated approaches to routing security, and data security at network layer. Here are some research topics and future work in the area. a) Cryptography is the fundamental security techniqueused in almost all aspects of security. The strength of anycryptographic network depends on proper key management. Thepublic-key cryptography approach relies on the centralized CA(certifying authority) entity, which is a security weak point inMANET. Some papers propose to distribute CA functionality tomultiple or all network entities based on a secret sharing scheme,while some suggest a fully distributed trust model, in the style ofPGP (Pretty Good Privacy).Since most attacks are unpredictable, a resiliency oriented security solution will be more useful, which depends on a multi-fence security solution.

REFERENCES

[1]. Y. Xiao, X. Shen, and D.-Z. Du (Eds.), “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, WIRELESS/MOBILE NETWORK SECURITY, 2006 Springer

[2]. C. Perkins, Ad Hoc Networks, Addison-Wesley, 2001.

[3]. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications, pp. 38-47, 2004.

[4]. M. Zapata, Secure Ad Hoc On-Demand Distance Vector (SAODV). Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.

[5]. Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On- Demand Routing for Ad Hoc Networks. Proc. of MobiCom 2002, Atlanta, 2002.

[6]. Y. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy, pp. 28-39, 2004.

[7]. B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of theACM Workshop on Wireless Security, pp. 21-30, 2002.

[8]. Y. Hu, APerrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks inWireless Ad Hoc Networks. Proc. of IEEE INFORCOM, 2002.

[9]. K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding- Royer, A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[10]. Khan, F., & Nakagawa, K. (2013). Comparative study of spectrum sensing techniques in cognitive radio networks. In *Computer and Information Technology (WCCIT), 2013 World*

Congress on (pp. 1-8). IEEE.

[11]. Khan, F., Bashir, F., & Nakagawa, K. (2012). Dual head clustering scheme in wireless sensor networks. In *Emerging Technologies (ICET), 2012 International Conference on* (pp. 1-5). IEEE.

[12]. Khan, F., Kamal, S. A., &Arif, F. (2013). Fairness improvement in long chain multihop wireless ad hoc networks. In *2013 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 556-561). IEEE.

[13]. Khan, F. (2014). Secure communication and routing architecture in wireless sensor networks. In *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)* (pp. 647-650). IEEE.

[14]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "PASCCC: Priority-based application-specific congestion control clustering protocol" Computer Networks, Vol. 74, PP-92-102, 2014.

[15]. Khan, S., & Khan, F. (2015). Delay and Throughput Improvement in Wireless Sensor and Actor Networks. In *5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)* (pp. 1-8).

[16]. Khan, F., Jan, S. R., Tahir, M., Khan, S., &Ullah, F. (2016). Survey: Dealing Non-Functional Requirements at Architecture Level. *VFAST Transactions on Software Engineering*, *9*(2), 7-13.

[17]. Khan, F., & Nakagawa, K. (2012). Performance Improvement in Cognitive Radio Sensor Networks. *the IEICE Japan*.

[18]. Khan, F., Khan, S., & Khan, S. A. (2015, October). Performance improvement in wireless sensor and actor networks based on actor repositioning. In *2015 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 134-139). IEEE.

[19]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network" in Trustcom/BigDataSE/ISPA, Vol.1, PP-318-325, 2015, IEEE.

[20]. Jabeen, Q., Khan, F., Khan, S., & Jan, M. A. (2016). Performance Improvement in Multihop Wireless Mobile Adhoc Networks. *the Journal Applied, Environmental, and Biological Sciences (JAEBS)*, *6(4S)*, 82-92.

[21]. Khan, F. (2014, May). Fairness and throughput improvement in multihop wireless ad hoc networks. In *Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on* (pp. 1-6). IEEE.

[22]. Khan, S., Khan, F., Arif, F., Q., Jan, M. A., & Khan, S. A. (2016). Performance Improvement in Wireless Sensor and Actor Networks. *Journal of Applied Environmental and Biological Sciences*, *6(4S)*, 191-200.

[23]. Khan, F., & Nakagawa, K. (2012). B-8-10 Cooperative Spectrum Sensing Techniques in Cognitive Radio Networks. *電子情報通信学会ソサイエティ大会講演論文集*, *2012*(2), 152.

[24]. Khan, F., Jan, S. R., Tahir, M., & Khan, S. (2015, October). Applications, limitations, and improvements in visible light communication networks. In*2015 International Conference on Connected Vehicles and Expo (ICCVE)*(pp. 259-262). IEEE.

[25]. Jabeen, Q., Khan, F., Hayat, M. N., Khan, H., Jan, S. R., &Ullah, F. (2016). A Survey: Embedded Networks Supporting By Different Operating Networks. *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN*, 2395-1990.

[26]. Jan, S. R., Ullah, F., Ali, H., & Khan, F. (2016). Enhanced and Effective Learning through Mobile Learning an Insight into Students Perception of Mobile Learning at University Level. *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN*, 2395-1990.

[27]. Jan, S. R., Khan, F., &Zaman, A. The perception of students about mobile learning at University level.

[28]. M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application," *Elsevier Future Generation Computer Networks (FGCS)*, "Accepted", 2016.

[29]. Jan, S. R., Shah, S. T. U., Johar, Z. U., Shah, Y., & Khan, F. (2016). An Innovative Approach to Investigate Various Software Testing Techniques and Strategies. *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN*, 2395-1990.

[30]. Khan, I. A., Safdar, M., Ullah, F., Jan, S. R., Khan, F., & Shah, S. (2016). Request-Response Interaction Model in Constrained Networks. *In International Journal of Advance Research and Innovative Ideas in Education, Online ISSN-2395-4396*

[31]. Azeem, N., Ahmad, I., Jan, S. R., Tahir, M., Ullah, F., & Khan, F. (2016). A New Robust Video Watermarking Technique Using H.

ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

264/AAC Codec Luma Components Based On DCT. *In International Journal of Advance Research and Innovative Ideas in Education, Online ISSN-2395-4396*

[32]. Jan, S. R., Khan, F., Ullah, F., Azim, N., &Tahir, M. (2016). Using CoAP Protocol for Resource Observation in IoT. *International Journal of Emerging Technology in Computer Science & Electronics, ISSN: 0976-1353*

[33]. Azim, N., Majid, A., Khan, F., Jan, S. R., Tahir, M., &Jabeen, Q. (2016). People Factors in Agile Software Development and Project Management. *In International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)* ISSN: 0976-1353

[34]. Azim, N., Majid, A., Khan, F., Tahir, M., Safdar, M., &Jabeen, Q. (2016). Routing of Mobile Hosts in Adhoc Networks. *In International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)* ISSN: 0976-1353.

[35]. *Azim, N., Khan, A., Khan, F., Majid, A., Jan, S. R., &Tahir, M. (2016) Offsite 2-Way Data Replication toward Improving Data Refresh Performance. In International Journal of Engineering Trends and Applications,* ISSN: 2393 – 9516

[36]. Tahir, M., Khan, F., Jan, S. R., Azim, N., Khan, I. A., &Ullah, F. (2016) EEC: Evaluation of Energy Consumption in Wireless Sensor Networks. . *In International Journal of Engineering Trends and Applications,* ISSN: 2393 – 9516

[37]. M. A. Jan, P. Nanda, M. Usman, and X. He, “PAWN: A Payload-based mutual Authentication scheme for Wireless Sensor Networks,” *Concurrency and Computation: Practice and Experience*, “accepted”, 2016.

[38]. Azim, N., Qureshi, Y., Khan, F., Tahir, M., Jan, S. R., &Majid, A. (2016) Offsite One Way Data Replication towards Improving Data Refresh Performance. *In International Journal of Computer Science Trends and Technology,* ISSN: 2347-8578

[39]. Safdar, M., Khan, I. A., Ullah, F., Khan, F., & Jan, S. R. (2016) Comparative Study of Routing Protocols in Mobile Adhoc Networks. *In International Journal of Computer Science Trends and Technology,* ISSN: 2347-8578

[40]. Tahir, M., Khan, F., Babar, M., Arif, F., Khan, F., (2016) Framework for Better Reusability in Component Based Software Engineering.*In the Journal of Applied Environmental and Biological Sciences (JAEBS)*, *6(4S)*, 77-81.

[41]. Khan, S., Babar, M., Khan, F., Arif, F., Tahir, M. (2016). Collaboration Methodology for Integrating Non-Functional Requirements in Architecture. *In the Journal of Applied Environmental and Biological Sciences (JAEBS)*, *6(4S)*, 63-67

[42]. Jan, S.R., Ullah, F., Khan, F., Azim, N., Tahir, M., Khan, S., Safdar, M. (2016). Applications and Challenges Faced by Internet of Things- A Survey. *In the International Journal of Engineering Trends and Applications,*ISSN: 2393 – 9516

[43]. Tahir, M., Khan, F., Jan, S.R., Khan, I.A., Azim, N. (2016). Inter-Relationship between Energy Efficient Routing and Secure Communication in WSN. *In International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)* ISSN: 0976-1353.