International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

MANET, Security Attacks and Routing Protocol: A Survey

Navanpreet Kaur[1], Harjit Singh[2]

[1]Student, Guru Nanak Dev University, RC Gurdaspur

[2]Assistant Professor, Guru Nanak Dev University, RC Gurdaspur

Abstract: ***MANET Stands for "Mobile Ad Hoc Network." A MANET is a type of ad hoc network in which mobiles are connected without wires. They use the wireless connections to connect to various networks. It can be Wi-Fi or other medium like satellite transmission. Mobile wirelesses networks are generally open to various attacks like information and physical security attacks than fixed wired networks. So, to get over these attacks CRN is implemented that stands for cognitive radio network. It will increase the security and performance of the network will be enhanced.***

Keywords: MANET, Malicious attack, cognitive radio network

1. Introduction

1.1 MANET

A MANET is a kind of specially appointed system that can change areas and design itself on the fly. Since MANETS are versatile, they utilize remote associations with interface with different systems. This can be a standard Wi-Fi association, or an alternate medium, for example, a cell or satellite transmission.[1]

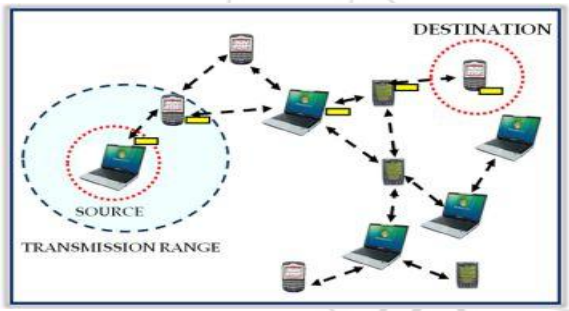

Figure 1.1: MANET

A few MANETs are confined to neighborhood remote gadgets, (for example, a gathering of smart phones), others may be associated with the Internet. For instance, A VANET (Vehicular Ad Hoc Network), is a kind of MANET that permits vehicles to speak with roadside gear. While the vehicles might not have a direct Internet association, the remote roadside gear may be associated with the Internet, permitting information from the vehicles to be sent over the Internet. The vehicle information may be utilized to quantify movement conditions or stay informed concerning trucking armadas. In view of the element nature of MANETs, they are normally not exceptionally secure, so it is vital to be careful what information is sent over a MANET.[1]

1.2 Security Attacks in MANET

- **Passive attack**: in this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping:
- **Denial of service attack:** Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.
- **Traffic Analysis:** In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information.[3,5]
- **Snooping**: It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.
- **Active attack:** in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker's threat can be performed [3].
- **Flooding attack:** In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power,

as well as network bandwidth will be consumed and could lead to denial-of-service.

- **Black hole Attack:** Route discovery process in AODV is vulnerable to the black hole attack. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough routes, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.[5]
- **Jamming:** Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets [4].
- **Malicious code attacks**: malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application. [2][3].

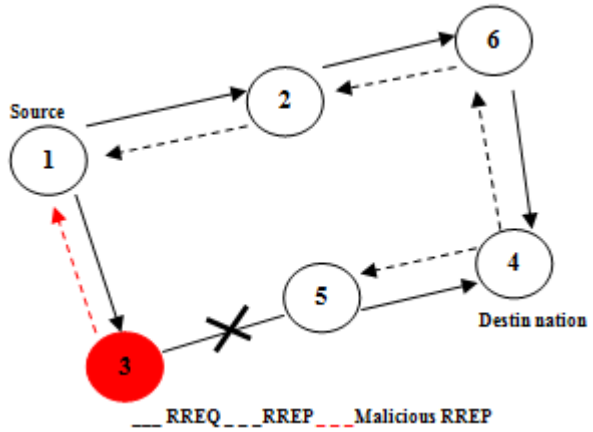

Figure 1.2: Malicious Attack

Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data transmissions.

Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage. Governments may snoop on individuals to collect information and prevent crime and terrorism. Although snooping has a negative aspect in general but in computer technology snooping can refer to any program or utility that performs a monitoring function [3].

2. Review of Literature

Burbank, J.L.et al [1] "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology" This article provides an overview of the military MANET problem space, describing the ideal military MANET solution. Several deficiencies are highlighted that exist between MANET technologies and the desired capability. Identified technical issues include system-level architecture, routing (both interior and exterior), management, security, and medium access control (MAC), with an emphasis on the former two areas.

Di Crescenzo, G.et al [2] "Securing reliable server pooling in MANET against byzantine adversaries" In this paper author secure the service discovery phase by using a secure multiple-dominating set creation protocol and the service provision phase by using a novel type of threshold signature scheme. Both protocols address novel security goals and are of independent interest as they can find applications to other areas; most notably, the construction of a distributed and survivable public-key infrastructure in MANET.

Dongkyun Kim.et al [3] "Improving TCP-Vegas Performance over MANET Routing Protocols" Recently, the Internet Engineering Task Force Mobile Ad Hoc Network (MANET) working group has standardized the reactive and proactive MANET routing protocols. In addition, work on using the transmission control protocol (TCP) to provide reliable data transmission has been performed for the purpose of smooth integration with the wired Internet. The authors propose their TCP-Vegas-ad hoc protocol, which is made aware of RCs and uses the correct BaseRTT values. Through simulations using ns-2, it was observed that the TCP-Vegas-ad hoc outperforms the standard TCP-Vegas protocol, especially under high mobility scenarios over both reactive and proactive ad hoc routing protocols.

Lee, Uichin. et al [4] "Efficient peer-to-peer file sharing using network coding in MANET" author in it argue that network coding in combination with single-hop communication allows P2P file sharing systems in MANET to operate in a more efficient manner and helps the systems to deal with typical MANET issues such as dynamic topology and intermittent connectivity as well as various other issues that have been disregarded in previous MANET P2P researches such as addressing, node/user density, non-cooperativeness, and unreliable channel. Via simulation, author show that our P2P protocol based on network coding and single-hop communication allows shorter file downloading delays compared to an existing MANET P2P protocol.

El Defrawy, K.et al [5] "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs" In this paper, author address a number of issues arising in suspicious location-based MANET settings by designing and analyzing a privacy-preserving and secure link-state based routing protocol (ALARM). ALARM uses nodes' current locations to securely disseminate and construct topology snapshots and forward data. With the aid of advanced cryptographic techniques (e.g., group signatures), ALARM provides both security and privacy features, including node authentication, data integrity, anonymity, and intractability (tracking-resistance). It also offers protection against passive and active insider and outsider attacks. To the best of our knowledge, this work represents the first comprehensive study of security, privacy, and performance tradeoffs in the context of link-state MANET routing.

Ziming Zhao.et al [6] "Risk-Aware Mitigation for MANET Routing Attacks" In this paper, author propose a risk-aware

response mechanism to systematically cope with the identified routing attacks. Our risk-aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factors. In addition, our experiments demonstrate the effectiveness of our approach with the consideration of several performance metrics.

3. Approaches Used

3.1 DSR: Dynamic Source Routing (DSR)

It is a reactive protocol i.e. it doesn't utilize occasional promotions. It figures the routes when important and after that looks after them. Source routing is a routing method in which the sender of a bundle decides the complete arrangement of hubs through which the bundle needs to pass; the sender expressly records this course in the bundle's header, recognizing each sending "hop" by the location of the following node to which to transmit the packet on its way to the destination host. There are two noteworthy stages in working of DSR: Route Discovery and Route Maintenance. A host starting a course disclosure telecasts a course ask for parcel which might be gotten by those hosts inside of wireless transmission scope of it. The course asks for bundle recognizes the host, alluded to as the objective of the course disclosure, for which the course is asked. On the off chance that the course disclosure is fruitful the starting host gets a course answer parcel posting an arrangement of system jumps through which it might achieve the objective. [5]

3.2 DSDV: The Destination-Sequenced Distance-Vector (DSDV)

Routing Algorithm depends on the traditional Bellman-Ford Routing Algorithm with certain changes. Each versatile station keeps up a steering table those rundowns all accessible destinations, the quantity of jumps to come to the destination and the arrangement number doled out by the destination hub. The arrangement number is utilized to recognize stale courses from new ones and in this manner keep away from the development of circles. The stations intermittently transmit their directing tables to their prompt neighbors. A station additionally transmits its directing table if a huge change has happened in its table from the last overhaul sent. There-fore, the upgrade is both time-driven and occasion driven. The steering table upgrades can be sent in two ways: a "full dump" or an incremental overhaul. A full dump sends the full directing table to the neighbors and could traverse numerous packets though in an incremental overhaul just those sections from the directing table are sent that has a metric change subsequent to the last redesign and it must fit in a packet.[4]

3.3 AODV

AODV: AODV offers low system use and utilizes destination arrangement number to guarantee loop opportunity. It is a reactive protocol suggesting that it demands a course when required and it doesn't keep up routes for those nodes that don't effectively partake in a correspondence. A vital component of AODV is that it utilizes a destination grouping number, which compares to a destination node that was asked for by a directing sender node. The destination itself furnishes the number alongside the route it needs to take to reach from the solicitation sender node up to the destination. In the event that there are various courses from a solicitation sender to a destination, the sender brings the route with a higher grouping number. This guarantees that the ad hoc network protocol remains loop free.[2]

3.4 Optimized Link State Routing (OLSR)

Protocol is a proactive routing protocol where the routes are continuously promptly accessible when required. OLSR is an advancement form of a pure link state protocol in which the topological changes cause the flooding of the topological data to every single accessible host in the system. OLSR might streamline the reactivity to topological changes by lessening the greatest time interim for occasional control message transmission. Besides, as OLSR ceaselessly looks after routes to all destinations in the system, the protocol is helpful for activity designs where an extensive subset of nodes are corresponding with another substantial subset of nodes, and where the [source, destination] sets are changing after some time. OLSR protocol is appropriate for the application which does not permit the long delays in the transmission of the data packets. The best workplace for OLSR convention protocol is a thick system, where the most correspondence is concentrated between substantial quantities of nodes.

OLSR diminish the control overhead driving the MPR to spread the upgrades of the connection state, additionally the effectiveness is picked up contrasted with traditional connection state convention when they chose MPR set is as little as conceivable. [3]

3.5 Temporally Ordered Routing Algorithm (TORA)

It is a very versatile, capable and adaptable conveyed routing algorithm taking into account the idea of connection inversion. Vital component of TORA is that control messages are limited to a little arrangement of nodes close to the event of a topological change. The convention has three key capacities: Route creation, Route upkeep and Route deletion. Route creation in TORA is made utilizing QRY and UDP parcels. The route creation algorithm begins by setting the stature of destination to 0 and for every single other node to NULL. The source telecasts a QRY parcel with the destination node's id in it. A hub with a non-NULL stature reacts with a UDP packet that has its tallness in it. A node getting a UDP packet sets its tallness is viewed as upstream and a node with lower stature downstream. Along these lines a coordinated acrylic diagram is developed from source to the destination. The resulting development of course on TORA is finished by exchanging demand from source and getting answer from destination.[3]

4. Conclusion

The dynamic topology character of MANETs makes it prone to various security attacks. Various attack include inside attacks and outside attack. A malicious attacker can rapidly

become a router and break network operations by deliberately not following the protocol specifications. Secure communication is an important aspect of any networking environment, is an especially significant challenge in ad hoc networks. In the work scenario is created of nodes, so to overcome this issue the protocol is used for communication of the nodes in it CRN, that is used for channel sensing. By using CRN security and performance of the network will enhance.

References

[1] Burbank, J.L. Johns Hopkins; Chimento, P.F. ; Haberman, B.K. ; Kasch, W. "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology" journal IEEE___on Communications Magazine, Volume 44, 2006,pp-39 – 45.

[2] Di Crescenzo, G. ; Telcordia Technol., NJ, Ge, R. ; Arce, G.R. "Securing reliable server pooling in MANET against byzantine adversaries" IEEE_Journal on Selected Areas in Communications, Volume 24 , 2006,pp- 357 – 369.

[3] Dongkyun Kim, Kyungpook Hanseok Bae. "Improving TCP-Vegas Performance Over MANET Routing Protocols"journal IEEE on Vehicular Technology, Volume 56, 2007,pp- 372 – 377.

[4] Uichin Lee, Joon-Sang Park, Seung-Hoon Lee, Won W. Ro, Giovanni Pau, Mario Gerla "Efficient peer-to-peer file sharing using network coding in MANET"IEEE Journal on Communications and Networks,Volume10, 2008,pp- 422 – 429.

[5] El Defrawy, K. Tsudik, G. "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs IEEE Journal on Mobile Computing, Volume10, 2010,pp-1345 – 1358

[6] Ziming Zhao; Security Eng. for Future Comput. Lab., Arizona State Univ., Tempe, AZ, USA ; Hongxin Hu ; Gail-Joon Ahn ; Ruoyu Wu "Risk-Aware Mitigation for MANET Routing Attacks" IEEE__Journal on Dependable and Secure Computing, Volume 9 , 2011,pp- 250 – 260.

[7] Shakshuki, E.M. Wolfville, NS, Canada, Nan Kang ; Sheltami, T.R. "EAACK—A Secure Intrusion-Detection System for MANETs" IEEE Journals on Industrial Electronics, Volume 60 , 2012,pp-1089 – 1098.

[8] Hiranandani, D. Santa Cruz, Santa CruzObraczka, K. ; Garcia-Luna-Aceves, J.J "MANET protocol simulations considered harmful: the case for benchmarking" IEEE Journal on Wireless Communications, Volume:20 , 2013 ,pp- 82 – 90.

[9] Bellavista, P. Bologna, Italy ; Cardone, G. ; Corradi, A. ; Foschini, L. "Convergence of MANET and WSN in IoT Urban Scenarios" IEEE_Journal on Volume 13 , 2013,pp-3558 – 3567.

[10] Gaeta, R. ; Dipt. di Inf., Univ. di Torino, Turin, Italy ; Grangetto, M. ; Loti, R. "Exploiting Rateless Codes and Belief Propagation to Infer Identity of Polluters in MANET" IEEE_Journal on Mobile Computing, Volume 13, 2013 ,pp- 1482 – 1494.