A STUDY ON SECURITY MECHANISM FOR MANET ROUTING

[1] V.Ramya, [2] B.Pavithra , [3] S.Tharani, [4] V.Uthra

[1] Assistant Professor [2] Assistant Professor, [3]Assistant Professor, [4]Assistant Professor
[1] Department of Computer science,
[1] Sri Ramakrishna College of Arts and Science for Women, Coimbatore-641006, TamilNadu, India.

Abstract : The Network called MANET (Mobile Ad-hoc Networks) which is designed for a special application, where it is not easy to use as a backbone network. The applications in the MANET are involved with sensitive and secrete information. For the major problem routing and security, the MANET assumes a trusted environment. In MANET, the proactive routing protocol called OLSR (Optimized Link State Routing) vulnerabilities is examined. It is analyzed with the variety of routing algorithms.

IndexTerms - MANET, routing protocol, community nodes, signature, information, Privacy.

I. INTRODUCTION

Past few years, have witnessed a rapid escalation in the field of mobile computing due to proliferation of inexperience, widely available wireless devices. Thus, it has opened vast opportunity for the researchers to work on Ad Hoc networks. In MANET, nodes within one another's wireless transmission range can communicate directly

1.1. Challenges in MANET

Almost every characteristics of the network has been explored to some level. Yet, no resolution to any of the problem has been found

- Routing in Dynamic Topology
- Topology maintenance (lack of central infrastructure)
- Scalability
- Energy Efficiency
- Security Privacy
- Autonomous
- Poor transmission Quality

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network.

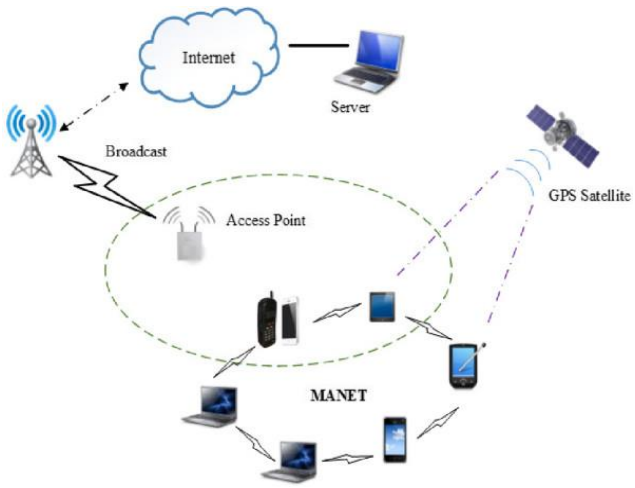

figure 1: manet architecture

II. REVIEW OF LITERATURE

The secure data sharing model on MANET is carried out using following privacy models

2.1 Detection of Malicious Packet Dropping in Wireless Ad Hoc Networks Based on Privacy-Preserving Public Auditing

Authors Bhagyashree S and Prof. Anand S Uppar says that Security is one of the most essential issues that have attracted a number of research and development effort in past few years. In multi-hop wireless advert hoc community link error and malicious packet losing are assets for packet losses. Whether the losses are due to link mistakes only, or with the aid of the mixed effect of link errors and malicious drop are to be diagnosed, can be known by means of staring at a series of packet losses in the network. But in the insider-assault case, wherein malicious nodes which are part of the direction take advantage of their know-how of the conversation context to selectively drop a small amount of packets crucial to the community performance.

2.2. ODSBR: An On-Demand Secure Byzantine Routing Protocol

Authors Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru y and Herbert Rubens says that not unusual method utilized by routing protocols for ad hoc wireless networks is to set up the routing paths on-call for, in place of always retaining a whole routing table. Since in an advert hoc community nodes no longer in direct variety talk via intermediate nodes, a sizeable subject is the potential to path in the presence of Byzantine failures which include nodes that drop, fabricate, alter, or mis-path packets in an attempt to disrupt the routing provider. It advise the primary on-call for routing protocol for advert hoc wireless networks that provides resilience to Byzantine screw ups as a result of individual or colluding nodes. The protocol is based on an adaptive probing approach that detects a malicious link after log n faults have happened, wherein n is the duration of the route. Problematic links are prevented by the usage of a weight-based totally mechanism that multiplicatively increases their weights and with the aid of using an on-call for direction discovery protocol that finds a least weight course to the vacation spot. Our protocol bounds the amount of harm that an attacker or a collection of colluding attackers can purpose to the network.

2.3. Short Signatures from the Weil Pairing

Authors Dan Boneh, Ben Lynn, and Hovav Shacham say that Short digital signatures are wanted in environments wherein a human is asked to manually key inside the signature. For example, product registration structures regularly ask users to key in a signature supplied on a CD label. More usually, short sig-natures are wanted in low-band width communication environments. For instance, quick signatures are wanted when printing a signature on a postage stamp. Currently, the 2 maximum regularly used signatures schemes, RSA and DSA, provide relatively lengthy signatures compared to the safety they provide. For instance, while one makes use of a 1024-bit modulus, RSA signatures are 1024 bits long. Similarly, while one makes use of a 1024-bit modulus, standard DSA signatures are 320 bits lengthy. Elliptic curve editions of DSA, along with ECDSA, also are 320 bits lengthy. A 320-bit signature is simply too lengthy to be keyed in with the aid of a human.

2.4. Malicious Node Detection System for Mobile Ad Hoc Networks

Authors A.Rajaram, Dr. S. Palaniswami, In this paper, the authors have proposed an initial technique to locate intrusions in ad hoc networks. Anand Patwardhan et al. [2] have proposed a secure routing protocol based totally on AODV over IPv6, in addition strengthened by way of a routing protocol impartial Intrusion Detection and Response device for ADHOC networks. Chin-Yang Henry Tseng [3] has proposed a complete disbursed intrusion detection gadget has consisted of 4 fashions for MANETs with formal reasoning. Tarag Fahad and Robert Askwith [4] have targeting the detection segment and they have proposed a mechanism Packet Conservation Monitoring Algorithm (PCMA) is used to hit upon egocentric nodes in MANETs.

2.5. Trust Value Algorithm: A Secure Approach against Packet Drop Attack in Wireless Ad-Hoc Networks

Authors Rajendra Aaseri, Pankaj Choudhary and Nirmal Roberts Says that Wireless ad-hoc networks are extensively used due to the fact those are very clean to set up. However, there are various protection problems and troubles. Two most crucial issues are interoperability and interaction amongst various safety technologies which are very important to don't forget for configuration and control factor of view. The packet drop ratio in the wi-fi community is very high as well as packets may be effortlessly delayed with the aid of the attacker. Ii could be very hard to discover intruders, so it results into high fake superb price. Packets can be dropped or not on time by means of intruders as well as outside nodes in wireless networks. Hence, there may be the need of effective intrusion detection system which could detect most wide variety of intruders and the corresponding packets be forwarded through some alternate paths within the community. In the proposed system it recommends the trade strategy to hit upon the intruders/adversary with assist of consider price. It would put off the need of built in IDS in the wi-fi networks and end result into enhancing the overall performance of WLAN.

2.6 . Packet Drop Attack in Wireless Ad-Hoc Network

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for discovery of a route to the goal in wireless ad-hoc networks [19]. When the source node requests to create an association with the destination node, it televises an RREQ message. In advert-hoc networks that appoint the AODV protocol, the intruder node sucks up the network passage and fall all the corresponding packets. To explain the Packet Drop Attack, It encompasses a malicious node that demonstrates Black Hole activities in the set-up. It assumes that Node three is the malicious node. When Node 1 televise the RREQ message for Node 4,

Node 3 immediately responds to Node 1 with an RREP message that comprise the maximum collection number of Node 4, as though it's far coming from Node 4. Node 1 presumes that Node 4 is following Node 3 with 1 hop and discards the lately arrived RREP packet coming from Node 2. Subsequently, Node 1 begin to discharge its records packet to the node 3 awaiting that those packets will arrive at Node 4 however Node three will drop all information packets. In a Packet Drop Attack, after a while, the beginning nodes recognize that there may be a linkage fault since the popularity node refusing to transmit TCP ACK packets. If it dispatch away fresh TCP facts packets and discover a sparkling route for the goal, the malicious node nevertheless takes care of to cheat the sending node. If the sending node releases UDP records packets, the difficulty isn't always diagnosed for the reason that UDP facts connections do not hang around for the ACK packets.

2.7. Mobile Ad Hoc Wireless Network

Authors Samba Sesay, Zongkai Yang and Jianhua He, says that the early advert hoc networking programs can be traced lower back to the DARPA (Defense Advanced Research Projects Agency) Packet Radio Network (PRNet) mission in 1972, which changed into primarily stimulated via the efficiency of the packet switching generation, which include bandwidth sharing and keep and-ahead routing and its feasible utility in mobile wireless surroundings. In PRNet community nodes and devices (repeaters, routers etc.) had been all mobile even though mobility was constrained.

2.8. Malicious Node Detection in Mobile Ad-Hoc Networks

Authors Dipali D. Punwatkar and Kapil N. Hande say that the hassle of protection and cooperation enforcement has acquired tremendous interest with the aid of researchers in the ad hoc network network. Watchdog and course rater [16] technique is proposed to locate and isolate the misbehaving nodes. In this approach, a node forwarding a packet tests if the next hop additionally forwards it. If no longer, a failure remember is incremented and the upstream node is rated to be malicious if the matter exceeds a certain threshold. The course rater module then makes use of this knowledge to keep away from it in direction selection. It improves the throughput of the community in the presence of malicious nodes. However, it has the demerit of no longer penalizing the malicious nodes.

2.9 . Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks

Authors Mike Just, Evangelos Kranakis and Tao Wan says that Most of the routing protocols in wireless advert hoc networks, which includes DSR, anticipate nodes are honest and cooperative. This assumption renders wi-fi advert hoc networks susceptible to diverse kinds of Denial of Service (DoS) attacks. It presents a allotted probing technique to detect and mitigate one type of DoS attacks, namely malicious packet dropping, in wi-fi advert hoc networks. A malicious node can promise to a head packets however in fact fails to do so. In our allotted probing technique, each node inside the community will probe the alternative nodes periodically to detect if any of them fail to carry out the forwarding characteristic. Subsequently, node nation information can be used by the routing protocol to skip those malicious nodes. Our experiments show that in a moderately converting community, the probing method can hit upon maximum of the malicious nodes with a notably low fake wonderful fee.

III. CONCLUSION

MANET is a very good architecture in wireless computing nowadays, because most of the wireless services are using MANET based devices, through this advantages and disadvantages, the researchers fall under conducted diverse techniques it proposes different types of malicious attacks, from that have to take the problem of Packet dropping attack and by preventing with the use of Optimized Link State Routing.

REFERENCES

[1] M. Chandra, “Extensions to OSPF to Support Mobile Ad Hoc Networking,” IETF Internet-draft, April, 2005
[2] T. Clausen, C. Dearlove, and P. Jacquet, “The Optimized Link-State Routing Protocol version 2,” IETF Internet-Draft, June, 2006.
[3] T. Clausen, C. Dearlove, J. Dean, and C. Adjih, “Generalized MANET Packet/Message Format,” IETF Internet-Draft, July, 2006.
[4] T. Clausen, and P. Jacquet, (eds.), “Optimized link state routing protocol (olsr),” IETF RFC 3626, 2003.
[5] R. Coltun, D. Ferguson, and J. Moy, “OSPF for IPv6,” IETF RFC2740, 1999.
[6] C. Crépeau, and C.R. Davis, “A Certificate Revocation Scheme for Wireless Ad Hoc Networks, Workshop on Security of ad hoc and Sensor Networks, 2003.
[7] C.R. Davis, “A localized trust management scheme for ad hoc networks,” International Conference on Networking (ICN’04), 2004.
[8] Y. G. Desmedt, “Threshold Cryptography,” European Transactions on Telecommunications, vol. 5, no. 4, July 1994, pp. 449-457.
[9] D. Dolev, and A. Yao, “On the security of public key protocols,” IEEE Transactions on Information Theory, Vol. 29, no 2, 1983, pp. 198-208.
[10] A.M. Hegland, P. Spilling, L. Nilsen, and Ø. Kure, ”Hybrid Protection of OLSR,” Workshop on Cryptography for Ad hoc Networks (WCAN’06)
[11] A.M. Hegland, E. Winjum, P. Spilling, C. Rong, and Ø. Kure, “Analysis of IBS for MANET Security in Emergency and Rescue Operations,” PCAC’06.

[12] A.M. Hegland, E. Winjum, S.F. Mjølsnes, C. Rong, Ø. Kure, and P. Spilling, "A Survey of Key Management in Ad Hoc Networks," To appear in IEEE Communications Surveys & Tutorials.
[13] Y. Khamayesh,R.Salah and M.B. Yassein. "Malicious Nodes Detection in MANETs: Behavioral Analysis Approach", Journal of Networks, Vol.7, No.1, January 2012.
[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", Proceedings of MobiCom 2000, August 2000.
[15] Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", IEEE 15th International Conference on Computer Modelling and Simulation, 2013.
[16] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof. J.S. Deshpande, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-407, 2010.
[17] Sumaiya Vhora, Rajan Patel, Nimisha Patel, " Rank Base Data Routing (RBDR) Scheme using AOMDV: A Proposed Scheme for Packet Drop Attack Detection and Prevention in MANET", IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015.
[18] Tao Shu and Marwan Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", IEEE Transactions On Mobile Computing, Vol. 14, No. 4, April 2015. [19] Raquel Lacuesta, Jaime Lloret, Miguel Garcia, and Lourdes, "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation", IEEE Transactions on Parallel And Distributed Systems, Vol. 24, No. 4, April 2013.
[20] Gavin Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In Tools and Algorithms for the Construction and Analysis of Systems (TACAS), volume 1055, pages 147–166. Springer Verlag, Berlin Germany, 1996.