International Journal of Pure and Applied Mathematics
Volume 116 No. 8 2017, 223-228
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

STUDY OF ROUTING ALGORITHMS AND ATTACKS ON ROUTING PROTOCOLS IN MANET

Ms. Mary Linda.I[1], Mrs. K. Shanmugapriya[2]
[1,2]Assistant Professor, Department of CSE,BIST,BIHER, Bharath University, Chennai-73
[1]Marylinda.cse@bharathuniv.ac.in

Abstract: A Mobile spontaneous Network (MANET) may be a assortment of wireless mobile nodes dynamically forming a short lived network while not the utilization of any existing network infrastructure or centralized administration. There are completely different routing protocols projected for MANETs that makes it quite tough to work out that protocol is appropriate for various network conditions .This paper provides associate study of various routing protocols. This paper presents a number of the offered secure routing protocols and most typical attack patterns against spontaneous networks. Routing protocols are subjected to case studies against the foremost usually known attack patterns such as: denial-of-service attack, tunneling, spoofing, part attack and hollow attack.

Keywords: MANETs, Routing Protocol, Security problems

1. Introduction

A wireless accidental network may be a decentralised variety of wireless network. The network is accidental as a result of it doesn't trust a pre-existing infrastructure, like routers in wired networks or access points in managed (infrastructure) wireless networks. accidental networks don't have an explicit topology or a central coordination purpose. Therefore, causation and receiving packets ar additional sophisticated than infrastructure networks[1-3].

Nowadays, with the Brobdingnagian growth in wireless network applications like hand-held computers, PDAs and cell phones, researchersar inspired to enhance the network services and performance. one amongst the difficult style problems in wireless accidental networks is supporting quality in Mobil Ad-hoc Networks (MANETs). The quality of nodes in MANETs will increase the quality of the routing protocols and therefore the degree of connection‟s flexibility. However, the pliability of permitting nodes to affix, leave, and transfer knowledge to the network create security challenges. A Manet may be a assortment of mobile nodes sharing a wireless channel with none centralized management or established communication backbone. Manet has dynamic topology and every mobile node has restricted resources like battery, process power and on-board memory. this type of infrastructure-less network is incredibly helpful in state of affairs within which standard wired networks isn't possible like battlefields, natural disasters etc. The nodes that ar within the transmission vary of every different communicate directly otherwise communication is finished through intermediate nodes that ar willing to forward packet therefore these networks also are referred to as as multi-hop networks.Mobile accidental network nodes arfurnished wireless transmitters and receivers victimization antennas, which can be extremely directional (point-to-point), position (broad-cast), in all probability manageable, or some combination[4-5]

2. Literature Survey

In MANETs, some kind of routing protocol is needed so as to dynamically observe the multi-hop ways through that packets is sent from one node to a different.

There area unit essentially 2 classes of routing protocols for MANETs:

2.1. Table Driven (Proactive): DSDV, GSR, WRP

2.2. supply Initiated On-Demand (Reactive): ABR, AODV, DSR, LAR.

2.3. Hybrid routing protocols: ZRP, SHARP

2.1. Proactive or Table-Driven RoutiIn

table driver routing protocols, each node maintains the constellation info, within the sort of routing tables by sporadically exchanging routing info.Routing info is mostly flooded within the whole network. Whenever a node needs a path to adestination, it runs Associate in Nursing applicable path finding rule on the topology info it maintains.ng Protocols[6]

2.1.1. Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV)

DSDV is developed on the idea of Bellman–Ford routing formula with some modifications. during this routing protocol, every mobile node within the network keeps a routing table. every of the routing table contains the list of all offered destinations and therefore the range of hops to every. every table entry is labeled with a sequence range, that is originated by the destination node. Periodic transmissions of updates of the routing tables facilitate maintaining the topology data of the network. If there's any new vital

modification for the routing data, the updates are transmitted like a shot. therefore the routing data updates would possibly either be periodic or event driven[6-8].

DSDV protocol needs every mobile node within the network to advertise its own routing table to its current neighbours. The advert is completed either by broadcasting or by multicasting. By the advertisements, the neighbouring nodes will realize any modification that has occurred within the network as a result of the movements of nodes. The routing updates may be sent in 2 ways: one is named a full dump and another is progressive. just in case of full dump, the whole routing table is shipped to the neighbors, wherever as just in case of progressive update, solely the entries that need changes ar sent.

2.1.2. Wireless Routing Protocol (WRP)

WRP belongs to the overall category of path-finding algorithms outlined because the set of distributed shortest path algorithms that calculate the ways victimization data relating to the length and second-to-last hop of the shortest path to every destination. WRP reduces the amount of cases during which a short lived routing loop will occur. For the aim of routing, every node maintains four things: one. A distance table a pair of. A routing table three.A link-cost table four. A message retransmission list (MRL)[9].

WRP uses periodic update message transmissions to the neighbors of a node. The nodes within the response list of update message (which is created victimization MRL) ought to send acknowledgments. If there's no amendment from the last update, the nodes within the response list ought to send associate idle hi message to make sure property. A node will decide whether or not to update its routing table when receiving associate update message from a neighbor and perpetually it's for a much better path victimization the new data. If a node gets a much better path, it relays back that data to the initial nodes in order that they will update their tables. when receiving the acknowledgment, the initial node updates its MRL. Thus, when the consistency of the routing data is checked by every node during this protocol, that helps to eliminate routing loops and perpetually tries to seek out out the simplest resolution for routing within the network[10].

2.2. Reactive or On-Demand Routing Protocol

Protocols that be this class don't maintain the topology data. They get needed|the mandatory} path once it's required, by employing a affiliation institution method. thence these protocols don't exchange routine data sporadically[11-13].

2.2.1. Dynamic Source Routing (DSR)

Dynamic supply Routing (DSR) may be a reactive protocol supported the supply route approach. In Dynamic supply Routing (DSR) protocol is predicated on the link state rule during which supply initiates route discovery on demand basis. The sender determines the route from supply to destination and it includes the address of intermediate nodes to the route record within the packet. DSR was designed for multi hop networks for tiny Diameters. it's a beaconless protocol during which no salutation messages square measure changed between nodes to give notice them of their neighbours within the network[14-15].

2.2.2. Ad Hoc on-Demand Distance Vector Routing (AODV)

AODV is essentially associate improvement of DSDV. But, AODV could be a reactive routing protocol rather than proactive. It minimizes the amount of broadcasts by making routes supported demand, that isn't the case for DSDV. once any supply node needs to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes successively broadcast the packet to their neighbors and therefore the method continues till the packet reaches the destination. throughout the method of forwarding the route request, intermediate nodes record the address of the neighbor from that the primary copy of the published packet is received. This record is hold on in their route tables, that helps for establishing a reverse path. If further copies of an equivalent RREQ square measure later received, these packets square measure discarded[16].

The reply is distributed exploitation the reverse path.For route maintenance, once a supply node moves, it will reinitiate a route discovery method. If any intermediate node moves among a selected route, the neighbor of the drifted node will discover the link failure and sends a link failure notification to its upstream neighbor. This method continues till the failure notification reaches the supply node. supported the received data, the supply would possibly plan to re-initiate the route discovery section[17]

2.2.3. Associativity-Based Routing (ABR)

ABR protocol defines a brand new kind of routing metric “degree of association stability” for mobile impromptu networks. during this routing protocol, a route is chosen supported the degree of association stability of mobile nodes. every node sporadically generates beacon to announce its existence. Upon receiving the beacon message, a neighbor node updates its own associativity table. for every beacon received, the associativity tick of the receiving node with the beaconing node is inflated. A high worth of associativity tick for any specific beaconing node means the node is comparatively static. Associativity tick is reset once any neighboring node moves out of the neighborhood of the other node[18].

2.3. Hybrid Routing Protocols

Protocols happiness to the present class mix the most effective options of the higher than 2 classes. Nodes among an explicit distance from the node involved or among a selected nation square measure aforesaid to be among the routing zone of the given node. For routing among this zone, a table-driven approach is employed. For nodes that square measure situated during this zone, square measure on-demand approach is employed[19].

2.3.1. Zone Routing Protocol (ZRP)

ZRP is appropriate for wide range of MANETs, particularly for the networks with giant span and various quality patterns. during this protocol, every node proactively maintains routes at intervals an area region, that is termed as routing zone. Route creation is completed employing a query-reply mechanism. For making completely different zones within the network, a node 1st must grasp UN agency its neighbors ar. A neighbor is outlined as a node with whom direct communication are often established, which is, at intervals one hop transmission vary of a node.Neighbor discovery info is employed as a basis for Intra-zone Routing Protocol (IARP). instead of blind broadcasting, ZRP uses question|a question |a question} management mechanism to cut back route question traffic by directional question messages outward from the query supply and far from coated routing zones. A coated node may be a node that belongs to the routing zone of a node that has received a route question[20].

During the forwarding of the question packet, a node identifies whether or not it's coming back from its neighbor or not. If yes, then it marks all of its well-known neighboring nodes in its same zone as coated. The question is so relayed until it reaches the destination. The destination successively sends back a reply message via the reverse path and creates the route[21].

2.3.2. Sharp Hybrid Adaptive Routing

SHARP adapts between reactive and proactive routing by dynamically variable the number of routing info shared proactively. This protocol defines the proactive zones around some nodes. the quantity of nodes in a very explicit proactive zone is decided by the node-specific zone radius. All nodes at intervals the zone radius of a selected node become the member of that specific proactive zone for that node. If for a given destination a node isn't gift at intervals a selected proactive zone, reactive routing mechanism (query-reply) is employed to determine the route to it node. Proactive routing mechanism is employed at intervals the proactive zone. Nodes at intervals the proactive zone maintain routes proactively solely with relevancy the central node. during this protocol, proactive zones square measure created mechanically if some destinations square measure oftentimes self-addressed or sought-after at intervals the network. The proactive zones act as collectors of packets, that forward the packets expeditiously to the destination, once the packets reach any node at the zone section.

3. Case Studies of Attack Patterns on Routing Protocols

There area unit quite range of routing protocols that area unit glorious in terms of potency. however the protection needs of those protocols modified things and a a lot of elaborated analysis is presently current to develop secure impromptu routing protocols. MANETs area unit very susceptible to attacks thanks to their dynamically dynamic topology, absence of typical security infrastructures and open medium of communication, which, not like their wired counterparts, can't be secured. to handle these considerations, many secure routing protocols are proposed: Secure economical Distance Vector Routing (SEAD), Ariadne, and attested Routing for impromptu Networks (ARAN), Secure impromptu On-Demand Distance Vector Routing (SAODV), and Secure Routing Protocol (SRP).

3.1. Secure Efficient Ad hoc Distance Vector (SEAD)

SEAD was developed supported Destination Sequence Distance Vector (DSDV) and incorporates unidirectional Hash operate to evidence within the routing update mechanism so as to boost the routing security. Securing a table driven protocol is more durable than securing associate on demand protocol because of the existence of predefined routes. Distance vector protocols encapsulate the route info into a hop count worth and a next hop. associate assailant cannot produce a legitimate route with a bigger sequence range that it received because of the properties of hash operate. As SEAD incorporates neighbor authentication through Hash functions, associate assailant cannot compromise any node. SEAD is prone through hollow attack. albeit authentication is provided mistreatment hash functions, a hollow attack is feasible through tunneling the packets from one location and retransmitting them from different location into the network.

All packets within the hollow attack flow during a circle rather than reaching the destination. Routing table overflow attacks area unit doable in SEAD, as SEAD is developed supported a table driven approach. A compromised node will advertise routes to nodes that aren't within the network and there by fill within the area allotted within the routing table with false node routes. Spoofing attack is feasible through compromised node acting sort of a destination node within the route discovery method by spoofing the identity of the destination node that may cause route destruction. part attack is additionally doable through a

compromised node advertising the shortest roots to non-existing nodes within the network. Tunneling and DOS attacks are doable through compromised nodes. Table driven protocols area unit way more vulnerable to security threats.

3.2. Ariadne

Ariadne was developed supported associate degree on demand protocol, Destination supply Routing (DSR). Ariadne uses MACs and shared keys between nodes to attest between nodes and use time stamps for packet period. hole attacks square measure potential in Ariadne through 2 compromised nodes. Ariadne prevents spoofing attacks with time stamps. the employment of supply routes prevents loops, since a packet passing through solely legitimate nodes won't be forwarded into a loop because of time stamps.

3.3. Secure Routing Protocol (SRP)

Secure routing protocol (SRP) was developed supported Destination supply Routing (DSR). The intermediate nodes taking part within the route discovery live the frequency of queries received from their neighbors and maintain a priority ranking reciprocally proportional to the question rate. therefore the malicious compromised nodes taking part within the network area unit given least priority to modify. the safety analysis is comparable to Ariadne because it relies on DSR protocol.

3.4. Authenticated Routing for Ad hoc Network (ARAN)

ARAN uses public key cryptography and a central certification authority server for node authentication and neighbor node authentication in route discovery. Denial-of-service attacks square measure potential with compromised nodes. Malicious nodes cannot initiate associate degree attack as a result of the neighbor node authentication through certificates. taking part nodes broadcast inessential route requests across the network. associate degree wrongdoer will cause congestion within the network, there by compromising the practicality of the network.

Spoofing attacks square measure prevented by ARAN through node level signatures. every packet within the network is signed by its personal key before broadcasted to ensuing level and checked for the authentication. thus spoofing the identity of node is hampered by ARAN. as a result of the sturdy cryptologic options of ARAN, malicious nodes cannot participate in any sort of attack patterns. solely compromised nodes will participate in any attack pattern. Tunneling attacks square measure potential in ARAN. 2 compromised neighbor nodes will collaborate to incorrectly represent the length of obtainable ways by encapsulating and tunneling the routing message between them. hole attack is additionally potential through 2 compromised nodes. Table overflow, part attacks square measure not possible as a result of node level authentication with signatures.

3.5. Secure Ad hoc On-Demand Distance Vector Routing (SAODV)

SAODV could be a wide enforced protocol in trade thanks to its robust security measures. SADOV uses a central key management in its routing topology. Digital signatures square measure accustomed demonstrate at node level and hash chain is employed to forestall the sterilization of node counts. Tunneling attacks square measure doable through 2 compromised nodes. hole attacks square measure perpetually doable with compromised nodes in any accidental constellation. the utilization of sequence numbers may stop most of the doable replay attacks.

4. Conclusion

In this paper variety of routing protocols for Edouard Manet, that ar broadly speaking categorised as proactive and reactive and Hybrid protocols. This paper discusses common attainable attacks on totally different protocols getting used in MANETs. We've got tried to investigate them thus on forestall the offender to intrude in wireless networks. There ar uncountable techniques with that, one will simply discover most of the attacks. One will opt for them in accordance with the protocol getting used within the network. However, no protocol is absolutely secure from attacks being encountered within the MANETs. Hence, one should opt for a mix of techniques showing intelligence to avoid any attack and create the network absolutely secure.

5. References

[1] Jayraj Singh, Arunesh Singh, Raj Shree "An Assessment of Frequently Adopted Security Patterns in Mobile Ad hoc Networks: Requirements and Security Management Perspective, Journal of Computer Science and Data Mining ,Vol. 1,No. 1-2,December 2011.

[2] Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. (pp. 2-17).

[3] Hao Yang, Haiyun Luo, Fan Ye, songwu Lu and LixiaZhang,"Security in mobile ad hoc networks: Challenges and solutions", IEEE Wireless Communications, Vol. 11, (2004) pp. 38-47.

[4] Hoang Lan Nguyen, UyenTrang Nguyen "A study of different types of attacks on multicast in mobile ad hoc networks", Journal of Ad hoc Networks, Vol. 6, (2006),pp. 32-46.

[5] Sudhir Agarwal, Sanjeev Jain, sanjeevSharma,"A survey of Routing attacks and security Measures in mibileadhoc networks", Journal of computing, Vol 3, Issue 1,(2011), pp. 41-48.

[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaelacardei,"A survey on Attacks and Countermeasures in Mobile ad hoc networks", Wireless/Mobile network security, Springer,(2006).

[7] Manel Guerrero Zapata, N. Asokan in Nokia research center and was submitted to WiSe'02, September 28, 2002, Atlanta, Georgia, USA".
[8] KimayaSanzgir, Bridget Dahilly, Brian Neil Levine, Clay Shields, Elizabeth M and Belding-Royer [2002]. "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02).
[9] Yih-Chun Hu, David B. Johnson and Adrian Perrig. "Secure Efficient Ad hoc Distance vector routing" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02).
[10] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and Secure Source Authentication for Multicast. In Network and Distributed System Security Symposium, NDSS '01, pages 35–46, February 2001.
[11]Ping Yi, Zhoulin Dai, YipingZhong, Shiyong Zhang [2005]. "Resisting Flooding Attacks in Ad Hoc Networks". Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (ITCC'05).
[12] AnandPatwardhan, Jim Parker and Anupam Joshi. "Secure Routing and Intrusion Detection in Ad Hoc Networks". [On-line] accessed on 6th November, 2005 at URL http://csrc.nist.gov/mobilesecurity/ Publications/ nist-umbc-adhocids-ipv6.pdf.
[13] PanagiotisPapadimitratos and Zygmunt J. Haas In Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.
[14] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.
[15] Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.
[16]Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.
[17]Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.
[18]Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.
[22]Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.
[23]Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.
[24]Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.
[25]Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.
[26]Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.
[27]R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)Volume 8, Issue 4, Pp. 376–385, April 2017.
R.Elankavi, R.Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.
R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.
[19]Thooyamani K.P., Khanaa V., Udayakumar R., Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, v-20, i-12, pp-2604-2612, 2014.
[20]Udayakumar R., Thooyamani K.P., Khanaa, Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, v-29, i-14, pp-19-24, 2014.
[21]Udayakumar R., Thooyamani K.P., Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, v-29, i-14, pp-6-10, 2014.