Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 6): pp.4172-4178
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.06.397

Critical Study Of Routing Protocols In Manets And Attacks On Manets

Abhay Raj Sahu Research Scholar, Department of Computer Application, Sri Satya Sai University of Technology & Medical Sciences, Sehore, M.P.

Dr. Jitendra Sheethlani Research Guide, Department of Computer Application, Sri Satya Sai University of Technology & Medical Sciences, Sehore, M.P.

ABSTRACT:

Ad hoc networks made up of mobile wireless nodes are known as MANETs. The network topology might alter over time since the nodes are mobile. Each node functions as a router, routing traffic throughout the network, and the nodes build their own infrastructure for the network. In order to forward packets to their destinations, MANET routing protocols must be able to adapt to changes in the network topology and maintain routing information. Although MANET routing methods are primarily for mobile networks, networks of stationary nodes without network infrastructure can also benefit from their use. Although there are more routing protocols that don't fall into either category, the two basic types of MANET routing protocols are reactive and proactive. When there is an immediate need for routing information, such as when one of the nodes needs to send a packet, reactive or on-demand routing protocols update it (and there is no working route to the destination). They then forward the payload after exchanging route discovery messages. The paths remain the same up until a packet's forwarding mistake. This paper reflects critical study of Routing Protocols

KEYWORDS: protocol, attacks, detect, malicious, algorithm, prevent

I INTRODUCTION:

Network security in MANETs is a major issue. Some of the attacks such as modification, impersonation, time to live and sleep deprivation are due to the misbehaviour of malicious nodes, which disrupts the transmission. Some of the existing security protocols such as ARAN, SAODV, SEAD etc., are basically used to detect and eliminate one or two types of attacks. The major requirement of a secure protocol is to prevent and eliminate many attacks simultaneously, which will make the MANETs more secure. The proposed algorithm can prevent and also eliminate multiple attacks simultaneously. This is called the MIST algorithm. This algorithm is written on the NTP based protocol, which provides the maximum utilization of the bandwidth during heavy traffic, with less overhead.

Malicious nodes can cause redirection of network traffic and denial of service (DoS) attacks by altering control message elds or by forwarding routing messages. The author (Siva Ram Murthy et al 2007), briefly discusses about several denial-of-service attacks against AODV and DSR protocols. Passive attacks include packet dropping to conserve resources. These abnormal node behaviors result in performance degradation and cause denial of service attacks, packet losses, longer delays, and low throughput. The effect of DoS attacks on MANETs can be serious, and the prevention and detection of these attacks is more difficult than in their wired counterparts.

II ROUTING PROTOCOLS:

Classification of Routing Protocols

Broadly, routing protocols for ad hoc networks can be classified into two broad classes: proactive protocols and reactive on-demand protocols that are discussed in the following sections (Siva Ram Murthy et al 2007).

Proactive protocols

The objective of proactive routing algorithms is to maintain consistent and up to-date routing information between every pair of nodes in the environment by proactively propagating route updates at predetermined constant time intervals. Generally, every node keeps this information in tables; hence, protocols of this genre are otherwise known as table-driven algorithms. Examples: Destination-Sequenced Distance Vector (DSDV), Topology-Based Reverse Path Forwarding (TBRPF) Protocols and Optimized Link-State Routing (OLSR) (Ade et al 2010). The DSDV protocol is a distance vector protocol that introduces extensions to make its operation suitable for MANETs. Every node maintains a routing table with one route entry provision for each destination, in which the shortest path route (based on the number of hops) is recorded. To avoid routing loops, a destination sequence number is used. A node increments its sequence number whenever a change occurs in its neighborhood. When given a choice between alternative routes for the same destination, a node always selects the route with the greatest destination sequence number. This ensures utilization of the route with the most recent information. The OLSR protocol is a variation version of the traditional link state protocol. An important aspect of OLSR is the introduction of multipoint relays (MPRs) to reduce the flooding of messages carrying the complete link-state information of the node and the size of link state updates. Upon receiving an update message, the node determines the routes (sequence of hops) to its known nodes. Each node selects its MPRs from the set of its neighbors such that the set covers those nodes that are distant two hops away. The idea is that whenever a node broadcasts a message, only those nodes present in its MPR set are responsible for broadcasting the message.

The Topology-Based Reverse Path Forwarding is also a variation of the link-state protocol. Each node has a partial view of the network topology, but is sufficient to compute the shortest path source spanning tree rooted at the node. When a node receives

source trees maintained at neighbouring nodes, it can update its own shortest path tree. TBRPF exploits the fact that shortest path trees reported by neighbour nodes tend to have a large overlap. In this way, a node can still compute its shortest path tree even if it receives partial trees from its neighbours. In this way, each node reports part of its source tree, called reported tree (RT), to all of its neighbours to reduce the size of topology update messages, which can be either full or differential. Full updates are used to send to new neighbours the entire RT to ensure that the topology information is correctly propagated. Differential updates contain only changes to RT that have occurred since the last periodic update. To decrease the number of control messages even further, topology updates can be combined with Hello messages so that fewer control packets are transmitted.

Reactive protocols

Reactive on-demand routing algorithms establish a route to a given destination only when a node requests it by initiating a route discovery process. Once a route has been established, the node keeps it until the destination is no longer accessible, or the route expires. Examples of reactive protocols are DSR and AODV (Sunil Taneja et al 2010). The DSR protocol determines the complete route to the destination node, expressed as a list of nodes of the routing path, and embeds it in the data packet. Once a node receives a packet it simply forwards it to the next node in the path. DSR keeps a cache structure (table) to store the source routes learnt by the node. The discovery process is initiated by a source node whenever it does not have a valid route to a given destination node in its route cache. Entries in the route cache are continually updated as new routes are discovered. Whenever a node wants to know a route to a destination, it broadcasts a RREQ message to its neighbours. A neighbouring node receives this message, updates its own table, appends its identification to the message and forwards it, accumulating the traversed path in the RREQ message. A destination node responds to the source node with a RREP message, containing the 10 accumulated source route present in the RREQ. Nodes in DSR maintain multiple routes to a destination in the cache, which is helpful in case of a link failure.

The AODV protocol keeps a route table to store the next-hop routing information for destination nodes. Each routing table can be used for a period of time. If a route is not requested within that period, it expires and a new route needs to be found when need arises. Each time a route is used, its lifetime is updated. When a source node has a packet to be sent to a given destination, it looks for a route in its route table. In case there is one, it uses it to transmit the packet. Otherwise, it initiates a route discovery procedure to find a route by broadcasting a RREQ message to its neighbours. Upon receiving a RREQ message, a node performs the following actions: checks for duplicate messages and discards the duplicate ones, creates a reverse route to the source node (the node from which it received the RREQ is the next hop to the source node), and checks whether it has an unexpired and more recent route to the destination (compared to the one at the source

node). In case those two conditions hold; the node replies to the source node with a RREP message containing the last known route to the destination.

III ATTACK:

Malicious nodes can cause redirection of network traffic and denial of service (DoS) attacks by altering control message elds or by forwarding routing messages with falsified values. The author (Siva Ram Murthy et al 2007), briefly discusses about several denial-of-service attacks against AODV and DSR protocols. Passive attacks include packet dropping to conserve resources. These abnormal node behaviours result in performance degradation and cause denial of service attacks, packet losses, longer delays, and low throughput. The effect of DoS attacks on MANETs can be serious, and the prevention and detection of these attacks is more difficult than in their wired counterparts.

3.1 Wormhole Attack

Packets are sent from one node in the network and tunneled to another node by the attacker. Routing can be disrupted when routing control messages are tunneled. Wormhole attacks (Khalil et al 2008) are severe threats to MANET routing protocols as they disrupt the flow of packets. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole or by isolating the malicious nodes using monitoring.

3.2 Black Hole Attack

The black hole attack exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Additionally, it consumes the intercepted packets without forwarding to the destined node. There is a more subtle form of these attacks when an attacker selectively forwards packets (Soufiene Djahel et al 2011). An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its misbehavior.

3.3 Byzantine Attack

A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

3.4 Rushing Attack

The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols. Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel

shared by attackers) exists between the two ends of the wormhole, the tunnelled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack.

3.5 Resource Consumption Attack

This is also known as the sleep deprivation attack. A compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

IV MIST ATTACK:

The MIST- NTP will completely secure the network against multiple attacks. The MIST security algorithm comprises of three algorithms, namely, the MDE, authentication algorithm, and self-recovery algorithm. Each algorithm in the MIST is explained briefly, for a better understanding of the overall working of the MIST-NTP.

4.1 Modification Attack:

Integrity (Stajano 1999) implies ensuring that the node has not been maliciously altered. In such cases, when the destination address of a node is tampered with, or maliciously altered, the node will start sending the packets to the modified destination node instead of the intended destination node. When this happens, there can be two fatal consequences: Initially, the intended node will not receive the packets so as to form a route during the initialization phase, and this consequently creates a break in the formation of the wireless topology. Secondly, this could even challenge the privacy of the data in the network, if the malicious node is successful in initiating the attack, and the entire network is attacked by the intruder. For convenience, the NTP is named as Malicious NTP (MNTP) when it gets attacked by the modification attack.

The following figure illustrate the actual path that has to be followed, and the path after malicious activity takes place, respectively. The intended route from Figure is 1-2-4-6 but due to malicious activity the destination is changed to 9, thus making the route 1-2-4-9. The data is sent to node 9 instead of node 6; thereby the data is lost due to lack of authenticity.

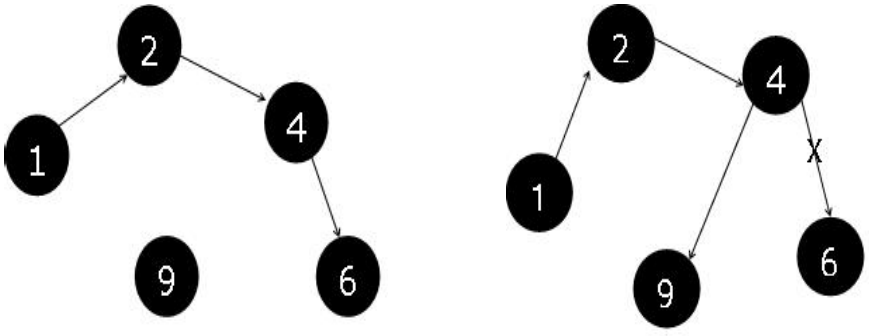

Figure : Before and After Malicious Activity

4.1.1 Malicious node detection and elimination (MDE):

For the detection and elimination of the malicious node which causes a modification attack, a novel algorithm named as the MDE scheme is used, that uses the beacon control packet of the NTP protocol. This is one of the modules in MIST algorithms.

The following are the steps implemented in the MDE algorithm, to detect and eliminate the malicious node in the network.

The malicious node (MN) address field is added to the beacon packet assuming that it is a non-mutable field, and hence, the information can only be updated and not altered. Also, the last address field in the beacon packet is assumed to be a nonmutable field.

When the node receives the beacon packet, it will compare the same with other beacon packets that it had received from its other neighbours. Using these received beacon packets, the node checks for any changes in the destination address of the packets it has received. The node also checks the flood number in the packet, for finding if there is really a malicious activity, or this is just a packet during connection establishment between the same source and a different destination. The new route discovery will have its flood number starting from one, whereas the maliciously altered packet will have a higher flood. This checking avoids false positives.

If the destination address of any one of the beacon packets has been changed by the malicious node, then node on receiving the beacon packet, the node will find the last address field (address of the previous node), from where the beacon packet has been received, and update the MN address field with the malicious node address in the last address field; which is shown in the following Figure.

Packet type	MN Address	Source Address	Destination Address	Last address	Last Node	Flood	Broadcast ID	Hop count

Figure: Beacon Packet with MN Address Field

On receiving the beacon packets from the neighbouring nodes, the nodes will update their neighbour tables by flushing the node corresponding to the MN address field, thereby eliminating the malicious node from the network. The use of a separate packet to notify the nodes about the malicious node, has been avoided by using an additional field (MN address) in the beacon packet itself. These costs a comparatively less overhead than the usage of a separate packet to notify in the network.

REFERENCES:

4177 | Abhay Raj Sahu Critical Study Of Routing Protocols In Manets And Attacks On Manets

Siva Ram Murthy, C. and Manoj, B.S. “Ad hoc Wireless Networks Architectures and protocols”, 2nd edition, Pearson Education, 2007

Stajano, F. and Anderson, R. “The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks”, Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, pp. 1-11, 1999.

Sunil Taneja and Ashwani Kush, “A Survey of Routing Protocols in Mobile Ad Hoc Networks”, International Journal of Innovation, Management and Technology, ISSN: 2010-0248, Vol. 1, No. 3, August 2010.

Yi, P., Dai, Z. and Zhang, S. “Resisting Flooding Attack in Ad Hoc Networks”, In Proceedings of IEEE Conference on Information Technology: Coding and Computing, Vol. 2, pp. 657-662, 2005.

Tameem Eissa and Shukor Abdul Razak, “Trust–Based Routing Mechanism in MANET: Design and implementation”, Mobile Network Applications–Springer, Vol online first, pp. 1-12, 2011.

Stajano, F. and Anderson, R. “The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks”, Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, pp. 1-11, 1999.

Hao Yang, Haiyunluo, Fan Ye, Songwulu and Lixia Zhng, “Security in Mobile Ad hoc networks: Challenges and Solutions”, IEEE Wireless Communications, pp. 38-47, 2004.

Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, “A Survey of Attacks and countermeasures in Mobile Ad Hoc Networks”, Mobile Network Security, pp. 1-38, 2006.