IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-2, Issue-4 E-ISSN: 2347-2693

A Survey of Source Routing Protocols, Vulnerabilities and Security in Wireless Ad-hoc Networks

Srihari Babu. Kolla[1*] and B.B.K. Prasad[2]

[1*,2] Dept. of Computer Science, Dhanekula Institute of Engg & Technology, India.

www.ijcseonline.org

Received: 24/03/2014 Revised: 10/04/2014 Accepted: 26/04/2014 Published: 30/04/2014

Abstract— A wireless Ad-hoc networks is the collection of wireless nodes that can co-operate by forwarding packets for each other to allow nodes to communicate directly. The deployment of Ad-hoc networks in security- and- safety in critical environments requires secure communication primitives. As WSN's become more and more crucial to everyday functioning of the people. Securing in wireless ad-hoc networks is a challenging task. Low power wireless networks are an existing research direction in routing and security. This paper discusses a wide variety of vulnerabilities while routing and different existing securities to mitigate them.

Keywords—Security, Vulnerabilities, WSN, Ad-Hoc Networks,Routing, Packet Forwarding

I. INTRODUCTION

Basically, a wireless Ad-hoc network is a challenging task. Ad-hoc network is a collection of nodes. In which individual nodes can co-operate by communicate each other. An ad-hoc network assumes that every node is also a router that can forward packets. As consequence, when two nodes are communicating all nodes in the vicinity of them must remain silent for the duration of communication. The deployment of wireless nodes where there is no infrastructure or the local infrastructure is not reliable can be difficult. As WSN'S become more and more crucial to everyday functioning of people. The main advantage of ad-hoc networks are flexibility, low–cost, robustness. Ad-hoc networks can be easily setup, even in desert places and can endure to natural catastrophes and war. Majority of the ad-hoc networks are deployed in hostile environments with active intelligent opposition. Hence security is a crucial issue. The design of a wireless ad-hoc network has to take into account several interesting and difficult problems. Wireless ad-hoc networks particularly vulnerable to attacks. These makes secure routing difficult task, because a adversary node can easily join the network and modify or fabricate routing information and impersonating other networks.

The basic contribution of this paper includes general vulnerabilities while routing and securities in wireless ad-hoc networks and finally how to mitigate those vulnerabilities. Section 2 gives the detailed routing protocols and types of protocols. Section 3 gives vulnerable attacks in ad-hoc networks and section 4 gives security for source routing protocols.

II. ROUING PROTOCOLS

A major challenge of wireless ad-hoc networks is the design of efficient routing protocols that can dynamically find routes between two communicating nodes. An ad-hoc routing protocol is a convention, or standard, that can controls, how nodes decide which way to route packets between nodes in network. Nodes in network are not familiar with the topology of their networks. Instead, they have to discover it. Typically a new node announces its presence to its neighbors. Each node knows about neighbors nearby and how to reach them, and may announce that it too can reach them.

In ad-hoc network nodes may move arbitrarily and the status of the communication links between the nodes is a function of several factors such as the position of nodes, the transmission power level, and the interference between neighbor nodes. Therefore, the mobility of nodes and the variety of the state of the links result in a network with fast and unpredictable topology changes. According to the routing strategy, ad-hoc routing protocols generally fall into two categories- those are topology-based and position based. Topology-based routing protocols find a route from source to destination according to the metrics of the network links. Networks that employ topology-based protocols forward packets based on the address of the destination node. Position-based routing protocols do not require the establishment or maintenance of routes. Here, the idea is to obtain the information about the geographical position of the destination and find the best way to forward packets to this position.

Topology-Based Routing

Topology-based routing protocols rely on the status of the network links to compute a route from a source to a destination. Thus, every node of the network has to exchange routing information to maintain routing tables up to date. Topology-based protocols can be further divided into proactive and reactive protocols. Proactive Routing Proactive routing protocols work like a classical Internet routing protocol. They share routing information even if there are no specific requests for a route to maintain consistent and up-to-date routes from each node to every other node in the

Corresponding Author: Srihari Babu. Kolla

network. Proactive protocols require that each node stores a routing table and responds to changes in network topology by propagating update messages throughout the network in order to maintain a consistent network state. This strategy continuously produces control traffic, which should be avoided for wireless networks. On the other hand, it provides low latency route access. The existing proactive protocols differ in the number of necessary routing-related tables and the methods by which changes in network topology are broadcasted. Examples of proactive protocols are DSDV and OLSR.

The Destination-Sequenced Distance-Vector (DSDV) routing protocol [1] is a modified version of the Bellman-Ford algorithm to guarantee loop-free routes. In DSDV, every node maintains a routing table in which the next-hop to all of the possible destinations is stored. The number of hops to each destination and a sequence number assigned by the destination node are associated to each routing table entry. The sequence numbers avoid the creation of routing loops once they enable the nodes to distinguish stale routes from new ones. Update packets are periodically sent throughout the network in order to maintain up-to date the routing tables of the nodes. In order to reduce the control overhead, two types of update packets are used: a full dump and an incremental packet. The full dump packet contains all the available information in the routing table of a node. On the other hand, the incremental packet carries only the information changed since the last full dump was transmitted. Although this mechanism reduces the routing overhead, as the topological changes increase, the number of incremental packets transmitted by DSDV also increases. In this situation, update routing packets use a large amount of network bandwidth.

The Optimized Link State Routing (OLSR) protocol [2, 3] is based on the link-state algorithm. In OLSR, each node periodically exchanges routing information with other nodes to maintain a topology map of the network. In order to reduce the flooding during the routing update process and the size of the update packets, OLSR employs multipoint relays (MPRs). In this mechanism, each node in the network selects a set of neighboring nodes to retransmit its update packets. For selecting the MPRs, a node periodically broadcasts *hello* messages to all one-hop neighbors to exchange its list of neighbors. From neighbor lists, a node calculates the nodes that are two hops away and computes the MPRs set which is the minimum set of one-hop neighbors required to reach the two-hop neighbors. The optimum MPRs computation is NP-complete [4], therefore heuristics are used by the OLSR protocol to compute the MPRs set. Each node notifies its neighbors about its MPRs set in the *hello* message. When a node receives the *hello*, it records the nodes that select it as one of their MPRs. These nodes are called MPR selectors. A routing update message transmitted by a node carries only information about its MPRs selectors. Thus, the size of a routing update message is reduced and a node can be reached only from its MPR selectors. The shortest path to a given destination is calculated using the topology map consisting of all of its neighbors and of the MPRs of all other nodes. The OLSR protocol is particularly suited for dense networks since if the network is sparse, most of the neighbors of a node becomes an MPR.

Reactive Routing Reactive, or on-demand, routing protocols operate only when there is an explicit request for a route. This strategy only creates routes when desired by a source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed when a route is found or when all possible route permutations have been examined. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible because a link ruptures or until the route is no longer needed. Reactive routing significantly reduces the memory consumption in the nodes and only generates control traffic when needed, but it typically floods the network with control messages to discover routes between two communicating nodes. In spite of providing fast route discovery, flooding has several inconveniences frequently observed, such as redundancy, contention, and collision. In a typical mobile ad hoc network, the resource consumption caused by control packets has a significant impact because of the low-bandwidth links and power-limited terminals. An example of reactive protocol is the Ad Hoc On-Demand Distance Vector (AODV) [5], which is based on the Bellman-Ford algorithm. In AODV, when a source node wants to send a packet to a destination and does not already have a valid route to that destination, the source initiates a route discovery process to find a route. Then, the source broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors. This process is repeated until either the destination or an intermediate node with a valid route to the destination is found. To guarantee that routes are loop free and contain the most recent information, AODV employs destination sequence numbers. Each node of the network maintains its own sequence number and a broadcast ID. Every time a node initiates a route discovery process, the broadcast ID is incremented. The address of the node and its broadcast ID uniquely identify an RREQ packet. The source also includes in the RREQ the most recent sequence number it has for the destination. Therefore, intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to the sequence number of the RREQ. When intermediate nodes forward RREQs, they record in their route tables the address of the neighbor from which the first copy of the RREQ packet is received, thereby establishing a reverse path. Due to the flooding process, other copies of the same RREQ can be received later and all are discarded. When the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or the intermediate node sends, in unicast, a route reply (RREP) packet back to the neighbor from which it first received the RREQ. As the RREP is routed back through the reverse path, nodes along this path set up forward route entries in their route tables.

There is a timer for each entry in the routing table, which limits the lifetime of unused routes. It is worth noting that AODV only supports symmetric links once the RREP is forwarded along the path previously established by the RREQ. AODV also employs a route maintenance mechanism. When a node within a route moves, its upstream neighbor notices the move and propagates a route error (RERR) message to each of its active upstream neighbors to inform them of the route rupture. These nodes in turn propagate the RERR packet to their upstream neighbors. This process is repeated until the source node is notified. Then, the source is able to initiate a new route discovery process for that destination. A link failure is detected using *hello* messages, which are periodically broadcasted to maintain the local connectivity of a node. Nodes can also detect a link failure by information from the data link layer.

The Dynamic Source Routing (DSR) [6] is another reactive protocol which is based on the strategy of source routing. In DSR, each node of the network maintains a route cache that contains the source routes of which the node knows. Entries in the route cache are continuously updated as the node learns new routes. DSR employs route discovery and route maintenance processes similar to AODV. When a node has to send a packet to a given destination, it first verifies its route cache to determine whether it already has a route to the destination. If it has a valid route to the destination, it will use this route to send the packet. Otherwise, if the node does not have a valid route, it initiates a route discovery process by broadcasting a route request packet. The route request contains the address of the destination, the address of the source node, and a unique identification number. Each node that receives the route request verifies if it knows a route to the destination. If it does not, it adds its own address to the route record field of the packet header and then forwards the packet to its neighbors. To limit the number of route requests propagated to its neighbors, a node only forwards the route request if the request has not yet been seen by the node and if the address of the node does not already appear in the route record. A route reply is generated when the route request reaches either the destination or an intermediate node, which contains in its route cache a valid route to the destination. When the route request reaches the destination or an intermediate node, it carries a route record containing the sequence of hops traversed. If the node that generates the route reply is the destination, it places the route record contained in the route request into the route reply. If the responding node is an intermediate node, it will append its cached route to the route record and then generate the route reply. In order to send the route reply, the responding node must have a route to the source. If it has a route to the source in its route cache, it may use that route. Otherwise, if symmetric links are supported, the responding node may reverse the route that is in the route record. If symmetric links are not supported, the node may initiate a new route discovery process and piggyback the route reply on the new route request. The asymmetric links support is an advantage of DSR as compared to AODV. DSR employs a route maintenance process based on route error messages. These messages are generated at a node when the data link layer detects a transmission failure. When receiving a route error, a node removes the failed node from its route cache and all routes containing the failed node are truncated at that point.

Position-Based Routing

Position-based routing protocols require that information about the geographical position of the communicating nodes be available. Each node determines its own position using GPS (Global Positioning System) or some other kind of positioning system [7]. In position-based routing, nodes have neither to maintain routing tables nor to exchange routing messages since the packet forwarding is performed based on the position of the destination node, carried by each packet. Then, before sending a packet, it is necessary to determine the position of its destination. Thus, the source node needs to use a location service to determine the position of the destination node and to include it in the destination address of the packet. In the following sections, we describe two position-based protocols, DREAM and Grid.

DREAM The Distance Routing Effect Algorithm for Mobility (DREAM) protocol [8] is an example of position-based protocol that employs an all-for-all location service. In DREAM, each node stores position information concerning every node of the network in a position database. An entry of this database contains a node identifier, the direction of and distance to a node, and a time value, which indicates the age of the entry. For propagating its position, a node periodically floods the network. The advantage of exchanging position information is that it consumes significantly less bandwidth than exchanging complete routing tables even if the network is flooded. The efficacy of network flooding can be improved according to two factors. The first one is that the frequency of position updates is a function of the mobility of nodes. Thus, a node can locally control the frequency at which it sends position updates according to its own mobility rate. The higher is the mobility of a node, the higher is the frequency of position updates. The second factor is the distance separating two nodes. The greater the distance separating two nodes, the slower they appear to be moving with respect to each other. This is called the distance effect [9]. Therefore, nodes in the direct neighborhood must exchange position updates more frequently than nodes farther away. A node can employ this strategy by indicating the distance that a position update can cover before it is discarded. The DREAM protocol also employs a restricted directional flooding to forward packets. A source sends a packet addressed to a certain destination to all its one-hop neighbors, which are within the direction toward the destination. In order to determine this direction, called the expected region, a node calculates the region where the destination is probably within. The expected region is a circle around the position of the destination node as it is known to the source. Since this position information may be

outdated, the radius r of the expected region is set to $(t1 - t0)$ $vmax$, where $t1$ is the current time, $t0$ is the timestamp of the position information of the destination which the source knows, and $vmax$ is the maximum speed that a node can move in the network. Given the expected region, the direction toward the destination can be defined. The neighboring nodes repeat this procedure using their information concerning the position of the destination. If a node does not have a one-hop neighbor in the required direction, a recovery procedure has to be initiated. This procedure is not implemented by DREAM.

Grid is a routing protocol [10, 11] composed by the Grid Location Service (GLS) and a greedy strategy for forwarding packets. The main idea of the Grid location service is to divide the area of an ad hoc network into several squares. Thus, GLS builds a hierarchy of squares where n-order squares contain four smaller $(n-1)$-order squares. An n-order square does not overlap other square of the same order. Every node of the network knows the hierarchy of squares and its origin. A node has a unique identification (ID) in the network defined by a hash function of one of its parameters such as the IP address or the MAC address. For identifying each node, GLS defines a circular identification space where the nearest ID of a given node is the smallest ID greater than the ID of the own node. For example, an ID space contains four IDs: 2, 12, 25, and 50. In this example, the nearest ID of 12 is 25 and the nearest ID of 50 is 2. A node periodically broadcasts update messages that contain its position and ID. These messages are limited to the first-square where the node is. Thus, each node only knows the position and the ID of its one-hop neighbors, which are within its first-order square. For disseminating its position through the network, first, a node sends an update message toward its three adjacent first order squares. Then, the nodes within these squares, which have the nearest ID of the transmitting node ID, are elected to store the position information of the transmitting node.

The Grid protocol uses the greedy strategy to forward packets. After finding the position of the destination, the source node sends a packet that carries this information to its closest one-hop neighbor to the destination. This process is repeated node-by-node until the destination receives the packet. Nevertheless, if there is no one-hop neighbor that is closer to the destination than the forwarding node itself, the packet forwarding fails. In this situation, an error message is returned to the source.

III. VULNERABILITIES IN AD-HOC NETWORKS.

Securing a wireless ad-hoc network is a challenging task. Eavesdropping in wireless communication is another threat usually impossible to detect. Multihop ad-hoc networks assume that every node is also a router that can forward messages. This makes secure routing difficult task because malicious node can easily join the network and modify or alter routing information. Several routing attacks are identified, such as –

Create routing loops: An adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. These strategies can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route.

Stretch attack: An adversary node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes.

Selective forwarding: An adversary selectively drops some packets.

Sinkhole: An adversary forges routing information claiming falsified shorter distances to attract packets and then discard some or all of them.

Black hole: A variation of sinkhole where all packets are discarded.

Warm hole: In the wormhole attack, an attacker records packets at one location in the network, tunnels them to another location, and retransmits them into the network

Isolation: An attacker forges routing information to cause a node to use a route detour preventing one set of nodes from reaching another.

Sybil attack: A single node duplicates itself and presented in the multiple locations. The Sybil attack targets fault tolerant schemes such as distributed storage, multipath routing and topology maintenance. In a Sybil attack, a single node presents a multiple identities to other nodes in the network.

Replication attack: an adversary may compromise a single legitimate node and insert copies throughout the network, increasing his presence in the network and thus allowing him to influence and subvert the network performance.

Jamming: An adversary may jam the radios of legitimate nodes in the network to prevent them from receiving important routing messages.

IV. SECURITY

PLGP [12] is another routing protocol that can provably resist from source routing protocol during the packet forwarding phase. The original version of the protocol, although designed for security, is vulnerable to warm hole attacks. So it can modify as PLGP with attestations (PLGPa). It uses packet history together with PLGP's tree routing structure. So every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet with traverses at least one honest node.

Several secure routing protocols were proposed. The Secure Efficient Ad Hoc Distance (SEAD) is a proactive secure routing protocol, based on the DSDV [13] protocol, that avoids modification of routing-table update messages. The basic idea is to use a one-way hash function to authenticate the sequence number and the metric fields of the messages.

The Secure Routing Protocol [14] is proposed to improve the DSR reactive protocol using an extension header that is attached to the route request and the route reply messages. A node that requests a route to a destination is able to identify and discard false routing information messages. Ariadne [15] is another secure protocol based on DSR and TESLA, which is an efficient broadcast authentication scheme that requires loose time synchronization. It assumes that each pair of communicating nodes has one secret key in each direction, and no assumption is made regarding the forwarding, which may exhibit malicious behavior.

To implement security in the AODV protocol, the Secure AODV (SAODV) protocol [16,17] was proposed. The authors assume that there is a key management system that makes it possible for each node to obtain public keys from the other nodes of the network, and that each node is capable of verifying the association between the identity of a given node and the public key of that node. Given these assumptions, the proposal secure important fields of the AODV messages. The SAODV uses a digital signature to authenticate the fixed fields of the messages, and hash chains to secure the hop count information, which is the only changeable information in the messages.

V. CONCLUSION

This paper summarizes source routing protocols, vulnerabilities and then how can we mitigate those vulnerabilities with existing protocols. Most of the proposals try to secure existing protocols and do not succeed against all possible attacks. Securing ad-hoc networks is still an open issue. Some researchers argue that all protocols for ad hoc networks must be designed thinking in security from the beginning. This survey will hopefully motivate future researchers to come up with smarter security and make network safer.

VI. ACKNOWLEDGEMENT

Most of all, I shall give all glory, honor and thank to my parents. They made me as I am. Then there are a few people I would like to thank, my well wishers and my guide Mr.B.B.k.Prasad , who spared no effort to ensure that I have everything I needed. Finally, the publisher and all the others who gave their time, love and energy.

REFERENCES

[1]. C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers," in ACM SIGCOMM, pp. 234–244, Aug. 1994.

[2]. T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)." IETF Request for Comments 3626, 2003.

[3]. T. Clausen, G. Hansen, L. Christensen, and G. Behrmann, "The optimized link state routing protocol, evaluation through experiments and simulation," in IEEE Symposium on Wireless Personal Mobile Communications, Sept. 2001.

[4]. L. Viennot, "Complexity results on election of multipoint relays in wireless networks," tech. rep., INRIA, France, 1998.

[5]. C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing." IETF Request for Comments 3561, 2003.

[6]. D. Johnson, D. Maltz, and J. Broch, DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks, ch. 5, pp. 139–172. Addison-Wesley, 2001.

[7]. J. Hightower and G. Borriello, "Location systems for ubiquitous computing," IEEE Computer, vol. 34, no. 8, pp. 57–66, Aug. 2001.

[8]. S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A.Woodward, "A distance routing effect algorithm for mobility (DREAM)," in ACM International Conference on Mobile Computing and Networking (MobiCom), (Dallas, USA), pp. 76–84, Oct. 1998.

[9]. S. Basagni, I. Chlamtac, and V. R. Syrotiuk, "Geographic messaging in wireless ad hoc networks," in Annual IEEE International Vehicular Technology Conference, (Houston, USA), pp. 1957–1961, May 1999. 32 Rubinstein et al.

[10]. J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris, "A scalable location service for geographic ad-hoc routing," in ACM International Conference on Mobile Computing and Networking (MobiCom), (Boston, USA), pp. 120–130, Aug. 2000.

[11]. R. Morris, F. Kaashoek, D. Karger, D. Aguayo, J. Bicket, S. Biswas, D. De Couto, and J. Li, "The grid ad hoc networking project." http://pdos.csail.mit.edu/grid/, 2003.

[12]. Byran Parno, Mark Luk, Evan Gaustad, and Aridane Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006

[13]. Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 3–13, June 2002.

[14]. P. Papadimitratos and Z. Hass, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), Jan. 2002.

[15]. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in ACM International Conference on Mobile Computing and Networking (MobiCom), pp. 12–23, Sept. 2002.

[16]. M. G. Zapata and N. Asokan, “Securing ad hoc routing protocols,” in ACM Workshop on Wireless Security (WiSe), pp. 1–10, Sept. 2002.
[17]. Neeraj Kumar Pandey and Amit Kumar Mishra, "An Augmentation in a Readymade Simulators Used for MANET Routing Protocols: Comparison and Analysis", International Journal of Computer Sciences and Engineering, Volume-02, Issue-03, Page No (60-63), Mar -2014

AUTHORS PROFILE

SRIHARI BABU.KOLLA is perusing Masters’ degree in computer science and engineering, JNTU KAKINADA. His research interested in network security, privacy and anonymity, low-power, security for sensor networks and mobile applications.

B.B.K Prasad is an associate professor in the department of computer science and engineering at Dhanekula institute of engineering and technology, India. He received his M.tech degree in computer science from RAJAN engineering college. His research interests include security for sensor networks and mobile applications, computer architecture, networks on chip.