RANDOMIZED ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS USING ALERT

[1]A.Rajeshkumar, [2]J.Rajesh kumar
[1]PG Scholar, Department of Computer science and engineering, RVS College of engineering and technology, Dindigul
[2]Assistant Professor, Department of Computer science and engineering, RVS College of engineering and technology, Dindigul
[1]rkfragile@gmail.com, [2]rajeshtween@yahoo.in

Abstract: Mobile ad hoc networks (MANETs) are infrastructure-less networks used in areas where rapid network configuration is needed, such as battle field communication. The lack of a trusted centralized authority, limited resources and the broadcast nature of wireless links make these networks susceptible to security threats. In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose an Anonymous Location-based and Efficient Routing protocol (ALERT). This anonymous location based approach hides the initiator or receiver information from the number of initiators or receivers in the system for providing the more security along the networks. This concept provides the protection to the source node, destination node and the forwarded node in the network. The anonymity protection is providing against the attacker or Sybil misbehavior. We use the EGPSR algorithm to find the best path between the source and destination nodes. After that we are calculate the RSS value for each node. Based upon the RSS value we identify the attacker nodes. We theoretically analyze the anonymity and efficiency of this network. We conduct the experiment against the theoretical value this shows, it provides the best anonymity and efficiency to the source and destination nodes as well as the routes. It requires low cost to provide this kind of a security.

1. INTRODUCTION

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes they, i.e., routing functionality will be incorporated into mobile nodes. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing.

However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

2. PROJECT SCOPE

- The main goal of this paper is effectively find the counter intersection and timing attacks.
- In this ALERT method to protection of sources, destinations, and routes.
- ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols.
- In this ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol.
- ALERT is strengthens the anonymity protection of

source and destination by hiding the data initiator/receiver among a number of data initiators/receivers.

- ALERT mainly uses randomized routing of one message copy to provide anonymity protection in low cost.

3. EXPERIMENTAL

To avoid the problem in existing system, we propose the new system is ALERT. In this work, the attackers can be battery powered nodes that passively receive network packets and detect activities in their vicinity. They can also be powerful nodes that pretend to be legitimate nodes and inject packets to the network according to the analytical results from their eavesdropped packets. ALERT find the Sybil attack misbehavior. We theoretically analyzed ALERT in terms of anonymity and efficiency. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/ receivers. We also conducted experiments to evaluate the performance of ALERT in comparison with other anonymity and geographic routing protocols. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base-line EGPSR (Energy Based Greedy Perimeter Routing) algorithm.

This ALERT concept uses the EGPSR algorithm to find the closet node in the network with the help of the energy of the node. For transmitting a packet in the network first we have to find the closet nodes which mean that source node, destination node and then the forwarded node. With the help of the forwarded node we send the packet to the destination in secure manner. We calculate the RSS value for each node. Based upon the RSS value we find that which node is attacker node. After that we start the packet transmission. The Sybil misbehavior can be identified and controlled in our proposed concept.

3.1 ADVANTAGES

- ALERT generates less cost due to encryption than ALARM and AO2P and overcome the Sybil misbehavior.
- ALERT achieves better route anonymity protection.
- It has significantly lower energy consumption.
- ALERT increases the possibility of packet delivery.

4. DESCRIPTION

4.1 EGPSR WITH SYBIL ATTACK DETECTION

Routing process is the process to find the nodes which are all involve in the particular area or zone. First Source node sends the routing packets to all the nodes involve in the simulation. Then find the destination node. All the nodes between the source node and the destination node make ready for transferring the packets.

4.2 RSS VALUE GENERATION

Each and every node calculates the RSS value for identifying the Sybil attack. RSS means that Received Signal Strength. These values are automatically calculated for each node. Each node has unique RSS value. Based upon the RSS value we identify the normal node and then the attacker node. The Normal node contains the low RSS value and the attacker node contains the high RSS value.

4.3 ENERGY BASED NODE SELECTION

After completing the routing process and RSS value generation, and then select the best path between the source node and destination node for packet transmission. Best path is finds out by the EGPSR routing algorithm. This EGPSR energy based routing algorithm finds out the forwarder node and relay node which have the high energy. ALERT varies depending on the randomly selected temporary destinations and the order of horizontal and vertical division, which provides a better anonymity protection.

4.4 SYBIL ATTACK DETECTION:

Before performing the transmission, first source node calculate the RSS value with the relay node. If the RSS value of the node is high, the node consider as the attacker node. If the RSS value of the node is low, the node consider as the normal node. If the node is normal node, source node is ready to communicate with node. From that information we efficiently find the Sybil attack.

4.5 PACKET TRANSMISSION:

After the completion of routing, then system makes the packet transmission between the source and destination. In this packet transmission period first, source node send the original packet to correct relay node and send dummy packets to remaining nodes. Then that relay node selects the random forwarder node and send the original packets. This type high energy node selection avoids the data losses. Again forwarder node act like the source node, that is send the original packet to the relay node and send the dummy packets to the other nodes. This process is continues up to the original packet reach the destination node.

5. ALGORITHMS

In our proposed concept use the EGPSR and GPSR routing algorithm to find the best path in our network. EGPSR – Energy based Greedy perimeter stateless routing. This EGPSR is used to find which node having the highest energy. That node is considered as a relay node between the source and destination. The relay node in the forwarded node sends the original packet to the destination node and then sends the dummy packets to the remaining nodes in the network. It is a routing principle that relies on geographic position information. Greedy forwarding tries to bring the message closer to the destination in each step using only local information. This algorithm finds the best path in the network using the energy of the node.

6. FEASIBILITY STUDY

6.1 Closet Node Selection

The MANET network contains the number of routing paths for transmitting the data. From this multiple path we have to choose or select the one best path with the help of the GPSR routing protocol. Select the best path between the source node and destination node for packet transmission. GPSR routing algorithm is used to find the closet node between source and destination node. This protocol finds the shortest path across the network. The shortest paths are fined with low cost and high latency.

In wireless networks comprised of numerous mobile stations, the routing problem of finding paths from a traffic source to a traffic destination through a series of intermediate forwarding nodes is particularly challenging. When nodes move, the topology of the network can change rapidly. Such networks require a responsive routing algorithm that finds valid routes quickly as the topology changes and old routes break. Yet the limited capacity of the network channel demands efficient routing algorithms and protocols that do not drive the network into a congested state as they learn new routes. The tension between these two goals, responsiveness and bandwidth efficiency, is the essence of the mobile routing problem.

Greedy Perimeter Stateless Routing, GPSR, is a responsive and efficient routing protocol for mobile, wireless networks. Unlike established routing algorithms before it, which use graph-theoretic notions of shortest paths and transitive reach ability to find routes, GPSR exploits the correspondence between geographic position and connectivity in a wireless network, by using the positions of nodes to make packet forwarding decisions. GPSR uses greedy forwarding to forward packets to nodes that are always progressively closer to the destination. In regions of the network where such a greedy path does not exist (*i.e.*, the only path requires that one move temporarily farther away from the destination), GPSR recovers by forwarding in perimeter mode, in which a packet traverses successively closer faces of a planar sub graph of the full radio network connectivity graph, until reaching a node closer to the destination, where greedy forwarding resumes. GPSR will allow the building of networks that cannot scale using prior routing algorithms for wired and wireless networks.

We assume the adversaries are able to perform both active and passive attacks to compromise the anonymity of the network on two levels: (1) to try to reveal identities of sender, receiver and en route nodes; (2) to try to link packets from the same communication flow. The attackers may also try to disrupt the routing process and manipulate data flows. We assume both external and internal adversaries exist in the network. An external adversary is a wireless node that can eavesdrop, record, alter and inject packets to carry out attacks like identity spoofing, link spoofing, replay attack, man-in-the-middle attack, etc. An internal adversary can be a compromised en-route node (or en-route insider) that possesses the necessary cryptographic secret to reveal the content of a packet and to generate legitimate messages.

Greedy forwarding's great advantage is its reliance only on knowledge of the forwarding node's immediate neighbors. The state required is negligible and dependent on the density of nodes in the wireless network, not the total number of destinations in the network. On networks where multi-hop routing is useful, the number of neighbors within a node's radio range must be substantially less than the total number of nodes in the network. The position a node associates with a neighbor becomes less current between beacons as that neighbor moves. The accuracy of the set of neighbors also decreases; old neighbors may leave and new neighbors may enter radio range. For these reasons, the correct choice of beaconing interval to keep nodes' neighbor tables current depends on the rate of mobility in the network and range of nodes' radios. We show the effect of this interval on GPSR's performance in our simulation results. We note that keeping current topological state for a one-hop radius about a router is the minimum required to do *any* routing; no useful forwarding decision can be made without knowledge of the topology one or more hops away.

A simple beaconing algorithm provides all nodes with their neighbors' positions: periodically, each node transmits a beacon to the broadcast MAC address, containing only its own identifier (*e.g.,* IP address) and position. The power of greedy forwarding to route using only neighbor nodes positions comes with one attendant drawback: there are topologies in which the only route to a destination requires a packet move temporarily farther in geometric distance from the destination.

6.2 SYBIL MISBEHAVIOUR

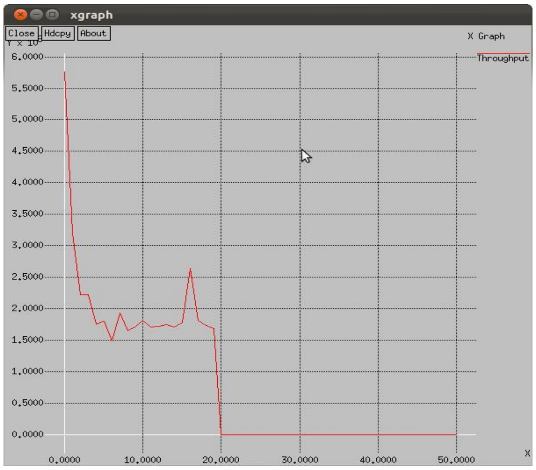
In our MANET network the possibilities of Sybil attack occurrences for loss the packet during the transmission. The Sybil attack creates the wrong identity to the source node and then loss the packet. During transmission, the Sybil attack gives wrong information to the source or relay node. In normal the relay node in the forwarded node is send the original packet to the destination zone. But in this Sybil attack, it does not provide the original packet to the destination. Sybil attack makes the more energy loss for the system. But our proposed concepts overcome the Sybil attack with the help of the EGPSR routing protocol. This selects the best path along the various paths in the network. These are all the processes are involved in the Sybil misbehavior concept or module.

In ad hoc networking, many systems apply redundant algorithms to ensure data flow from one node to another. So it may be difficult for the attackers to destroy the integrity of information. If the same packet is sent over several distinct paths, a change in the packet can be detected easily and the suspected intruder may be isolated. On the other hand, if the pieces of related information are sent on several distinct routes, an eavesdropper might have difficulties in putting together all the pieces of information to the destination.

However, if a single malicious node in a network represents several other nodes, as in the case of Sybil attack, the efficiency of the aforesaid attack detection technique reduces significantly. In this case, the destination node may not be able to detect the tampering because the attacker may get access to all pieces of fragmented information or may alter all the packets toward the same destination. This type of attack may be prevented or traced by legitimate nodes only if the nodes are cryptographically authenticated. Sybil attacker presents multiple identities simultaneously or exclusively. We consider the impact of Sybil attack to be at network and application layer levels. The network must ensure that distinct identities refer to distinct entities at different levels in the network. The difference between network layer and application layer is that each entity can show multiple identities simultaneously in the application layer, whereas multiple identities cannot be shown simultaneously in the case of network layer; rather it can be shown exclusively in this case. From the network layer point of view, IP address may be considered as the identifier of a node.

7. GRAPH CONSTRUCTION

In NS2, we have to show the energy details in the graph. This with Sybil attack contains the low energy level. These values are compared with the theoretical value. The half of the energy level will be reduced.



8. LIMITATIONS

There is no dynamic window advertisement, segment and ACK number computations are in units of packets, and there is no SYN/FIN connection establishment/teardown. The simulator models for Reno, NewReno, Sack, and Fack TCP are described briefly in Section 17.1.5 of the *ns Manual.* The one-way implementation in the simulator also does not have the sender check that the receiver is ECN capable, as would be done in a real implementation. The two-way TCP (FullTCP) does.

9. CONCLUSION

In mobile ad hoc networks the data's or packets are transferred between the source and destination nodes. The possibilities of Sybil attack in our network. In order to provide security and then overcome the problems presented in existing system, we introduce new concept called ALERT (An Anonymous Location based Efficient Routing Protocol). In our proposed concept first selects the node for packet transmission. This means, we select the source node, destination node and forwarded node. After that we select the random forwarded node for packet transmission. But the Sybil attack can create the wrong identities for a node for packet loss. In order to provide the security we introduce the GPRS routing protocol to find the best path in our network for packet transmission.

The GPSR select the relay for packet transmission. The source first send the data to the random forwarded node, that node sends the packet to the relay in destination zone. This relay node sends the original packet to the destination node and sends the dummy node to the remaining node in the network. This process is continuous until the packet receives the destination node. Finally we construct a graph from the received data and then compared with the theoretical values. This system provides the efficiency and requires low cost for hide the initiator/ receiver identities.

REFERENCE

[1] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT), 2006.

[2] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.

[3] V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.

[4] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.

[5] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.

[6] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[7] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K.Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J.Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[8] X. Wu, J. Liu, X. Hong, and E.Bertino, "Anonymous Geo- Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.

[9] Debian Administration, http://www.debian-administration.org/ users/dkg/weblog/48, 2012.

[10] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks:

[11] Research Articles," Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006.