International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015
ISSN 2091-2730

DETECTION OF INTRUDER NODES IN AUTONOMOUS MOBILE MESH NETWORKS

* Kiruthika Devi. M, Rama Rajan

*M.E Applied Electronics, Sri Eshwar College of Engineering, Coimbatore.

Project Engineer, VESTAS Power system

Abstract— In this paper, we describe the Autonomous Mobile mesh network with security. In MANET nodes move from one place to another place in free directions. The movement of the nodes may split the network and form more than one group. In this case communication between two nodes will be disconnected. To maintain the communication between all nodes even they are in different groups Mesh Nodes are used. Mesh Nodes which have the capability of changing its nature into Inter-group router or Intra-group router. Even it can act as a bridge router. To make the communication effective One-hop neighbor information update is used to find the shortest path between any two nodes. Since nodes move from one place to another place intruder may join the group. To avoid this problem private key is assigned for all the nodes in the network and it is shared among the nodes. If any node want to communicate with the other node first private key must be exchanged. Only if private key matches nodes can communicate. If key does not matches then the node ID will be registered in the Blacklist. If any node registered in the blacklist says the private key wrongly, then the node will be removed from the network. In this way security can be provided to the network.

Keywords— adhoc network, quality of service, MANET,AMMNET, location tracking, network security, group key management

INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks and enterprise installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level of the OSI model network structure. Examples of wireless networks include cell phone networks, Wi-Fi local networks and terrestrial microwave networks.

Wireless technology has been one of the most transforming and empowering technologies in recent years. In particular, mobile ad hoc networks (MANETs) are among the most popularly studied network communication technologies. In such an environment, no communication infrastructure is required. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless.

This paper proposes a mechanism that allows non-GPS-equipped nodes in the network to derive their approximated locations from a limited number of GPS-equipped nodes In our method, all nodes periodically broadcast their estimated location, in term of a compressed particle filter distribution. Non-GPS nodes estimate the distance to their neighbors by measuring the received signal strength of incoming messages. A particle filter is then used to estimate the approximated location from the sequence of distance estimates.

Typically, routing protocols are classified according to the route discovery philosophy, into either reactive or proactive. Reactive protocols are on-demand. Route-discovery mechanisms are initiated only when a packet is available for transmission, and no route is available. On the other hand, proactive protocols are table-driven. Routes are pre-computed and stored in a table, so that route will be available whenever a packet is available for transmission.

Ad hoc networking is an attractive concept and has various possibilities for different kinds of applications. In some application environments, such as battlefield communications, disaster recovery etc., the wired network is not available and multi-hop wireless networks provide the only feasible means for communication and information access. This kind of network is called Mobile Ad hoc network (MANET). It is also expected to play an important role in civilian forums such as campus recreation, conferences, and electronic classrooms etc. A MANET can be seen as an autonomous system or a multi-hop wireless extension to the Internet. As an autonomous system, it has its own routing protocols and network management mechanisms. As a multi-hop wireless extension, it should provide a flexible and seamless access to the Internet.

RELATED WORK

Mobile ad hoc networks (MANET) are constructed on-the-fly as nodes move in and out of the transmission range of each other. A major challenge in protocol design for MANETs is to provide mechanisms that deal with this dynamic topology change. Constant topology change has an inverse effect on fundamental tasks such as routing since routing algorithms cannot simply rely on previous knowledge of the network topology. Furthermore, even after a route has been successfully established, it can still be disrupted at any time due to the movement of the intermediate nodes. For this reason, most protocols originally designed for static networks cannot be adopted to ad hoc networks without significant change. Thus, many protocols have to be redesigned for ad hoc networks in order to cope with the topology change.

One great challenge in designing robust MANETs is to minimize network partitions. As autonomous mobile users move about in a MANET, the network topology may change rapidly and un-predictably over time; and portions of the network may intermittently become partitioned. This condition is undesirable, particularly for mission-critical applications such as crisis management and battlefield communications. We address this challenging problem in this paper by proposing a new class of robust mobile ad hoc network called Autonomous Mobile Mesh Networks (AMMNET). The AMMNET has the following additional advantages. The mobility of the mesh clients is confined to the fixed area serviced by a standard wireless mesh network due to the stationary mesh nodes. In contrast, an AMMNET is a wireless mesh network with autonomous mobile mesh nodes[1].

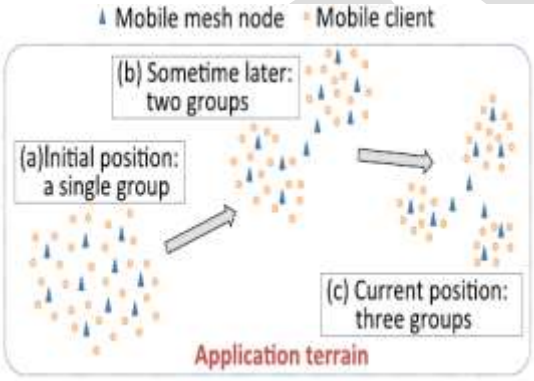

Fig.1. Partition and its topology adaptation

We classify the works related to AMMNET into three categories: 1) stationary wireless mesh networks: AMMNET is a new type of mesh networks, but supports dynamic topology adaptation, 2) sensor covering: the techniques for sensor covering is related to the design of covering mobile clients in AMMNET, and 3) location tracking: tracking mobile clients in AMMNET is an application of location tracking.

Given a network graph $G = (V,E)$ in which the number of location-aware nodes (also called *anchor* nodes) $|Vgps| \cdot |V|$, the objective of the location tracking algorithm is to find the locations of *non-anchor* nodes $\{V\} - \{Vgps\}$. In this section we survey the previous work on the location tracking problem in ad hoc networks.

The algorithms listed earlier all rely on the availability of reasonably accurate location information. This assumption is valid for networks in which some location sensing devices, such as GPS receivers, are available at all nodes. However, in reality this is rarely the case; although GPS receivers are increasingly cheaper to produce and becoming more widely available [6], they are still relatively expensive and power-hungry, and it is too general to assume that they will be available to every node in ad hoc networks. For this reason, different algorithms have been proposed to derive approximated locations of all nodes based on the relaxed assumption that direct location sensing devices are available to some nodes.

ONE-HOP ROUTING

To make the communication effective One-hop neighbor information update is used to find the shortest path between any two nodes. For communication between the nodes or between groups initially the source enables the route discovery process to find the shortest path based on one hop neighbor information.

Algorithm

Step 1: Nodes share and store information (id, position, distance, mobility) of its neighbors who are in closer than others in its coverage range.

Step 2: Source enables route discovery process. While receiving discovery packet each node forwards to its one hop neighbors.

Step 3: source receives acknowledgement (intermediate hop ids, distance) from intermediate hops(relays) and destination.

Step 4: source finds shortest path by received acknowledgement from destination.

Step 5: Sends data through that path.

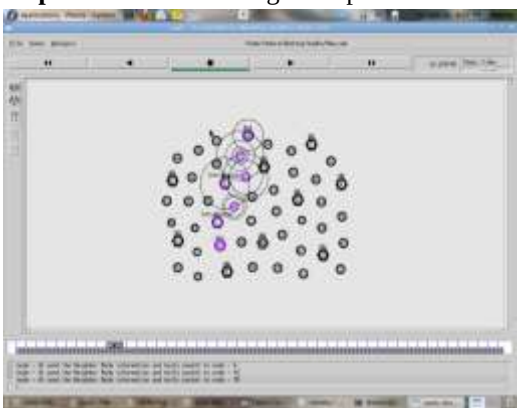

Fig.2. communication inside the group

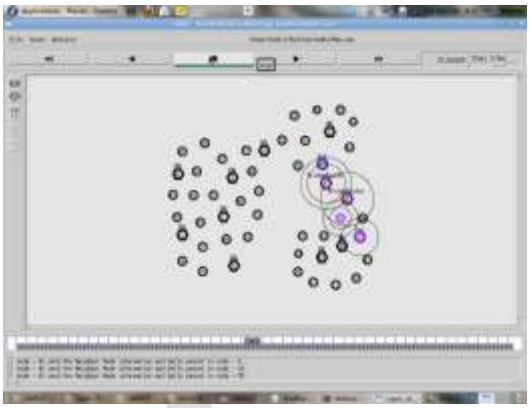

Fig.3. communication between the group

LOCATION TRACKING

This paper presents a solution to the location tracking problem based on particle filters. Given an ad hoc network with limited number of location-aware nodes, our solution estimates the locations of all other nodes by measuring the received signal strength indication (RSSI) from neighbors. For each node, the estimated location is viewed as a probabilistic distribution maintained by a particle filter. Unlike other location tracking methods, our solution has low overhead because it is purely based on local broadcasting and does not require flooding of the location information over the entire network[11]. Simulation studies show that even without flooding, our solution can still generate good estimates comparable to other existing methods, given that the network is well connected and the percentage of anchors is not extremely low. In addition when connectivity is low and the percentage of anchors is small, our algorithm is still able to derive location information which is not the case with most of the other approaches.

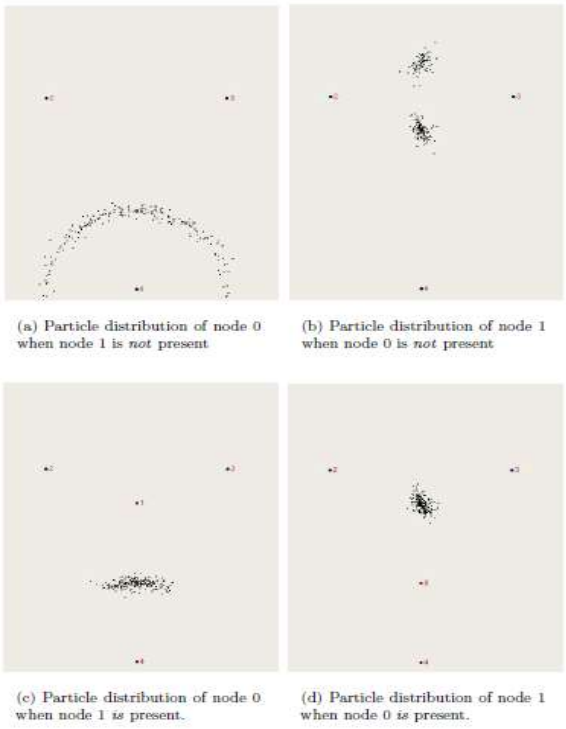

Fig.4. Location distributions in simple ad hoc scenarios

Generally speaking, there are two categories of localization methods depending on whether sensory data are used. The methods that do not use sensory data are simpler but tend to perform poorly especially when anchor ratio is low or the network is [12] sparse. The methods that do use sensory data generally perform better but tend to be significantly more complex. The performance in the latter case is also largely affected by the noise introduced to the sensory data which tends to aggregate rapidly as sensory data is propagated through the network.

Figure 4 demonstrates how our method solves the localization problem in a simple scenario. Here, nodes 2, 3 and 4 are GPS nodes, and node 0 and 1 are non-GPS nodes. Of the non-GPS nodes, node 0 may receive signals from nodes 1 and 4, and node 1 may receive signal from nodes 0, 2, and 3. The probability distribution of the estimated location is represented by the particles in the graph. In case (a), node 0 can only receive a signal from node 4. Thus, as the particle densities indicate, the probability distribution of node 0's location is on a circle around node 4. In Figure 1(b), node 1 can receive signals from node 2 and 3. Thus, node 1 is probably located where circles around nodes 2 and 3 intersect. Intuitively, in order to localize itself a node needs to receive location information from a minimum of three other nodes. In both case (a) and case (b), the location of nodes 0 and 1 cannot be derived because they do not receive location information from three other nodes. In Figures 1(c) and (d), node 0 and 1 are able to communicate to each other and exchange their probability distributions. Thus, their locations can be identified even though neither node receives location information from all three GPS nodes directly.

Fig.5. Node Movement Fig.6. Star Formation Fig.7. Track the node

SECURITY

Group communications are created all over the network in the form of videoconferences, on-line chatting programs, games, and gambling. Security plays an important role in these instances of group communication. According to [13], member authentication processes and key distribution take place at the beginning of a group communication. The group size tends to be less than 100 [14]. However, the Group Key (GK) generation takes a relatively long time to complete. For achieving a high level of security, the GK should be changed after every member joins and leaves so that a former group member has no access to current communications and a new member has no access to previous communications [13]. The group key agreement protocol focuses on the GK generation, which consists of evaluating a function of modular exponentiations.

The idea of the proposed algorithm relies on the premise that the members in the distributed computing do not have equal computing power. The higher the level in the key generation tree needs to longer time to compute the key. The key node <0,0> is taking more computation times than any other nodes' computations. Fig. 2 illustrates the reordering of members in the key generation tree.

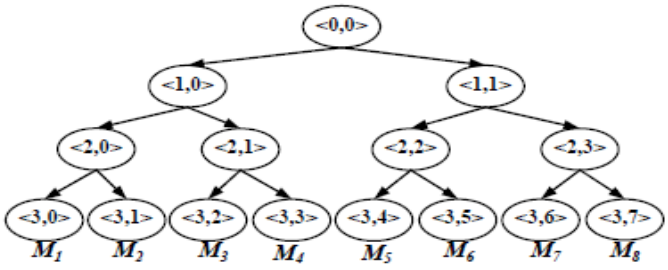

Fig.8. Reordering of Members in the Key Generation Tree

To illustrate the reordering mechanism an eight-member tree as shown in Fig. 2 is used. The leaf nodes represent members (M_1, M_2, M_3, M_4, M_5, M_6, M_7, and M_8). The sibling nodes in the tree are $<M_1, M_2>$, $<M_3, M_4>$, $<M_5, M_6>$, and $<M_7, M_8>$. Each member generates a secret key and calculates a blind key. Also he/she measures the elapsed time for generating the keys, and then each member starts to exchange their keys using the Diffie-Hellman key exchange. For example, M_1 and M_2 exchange the public keys $BK_{<3,0>}$ ($g_{K<3,0>}$ mod p) and $BK_{<3,1>}$ ($g_{K<3,1>}$ mod p) to generate sub-group key $g_{K<3,0>K<3,1>}$ mod p. Other sibling nodes ($<M_3, M_4>$, $<M_5, M_6>$,

and <M_7, M_8>) exchange their blind keys as the same wayM_1 and M_2 did. After completing the leaf level computation, the next level in the key tree is ready to be calculated. A Group Controller (GC) who is the last member to join the group determines which member goes to the next level with comparing each member's elapsed times, $T_c(M_{<l, v>})$.

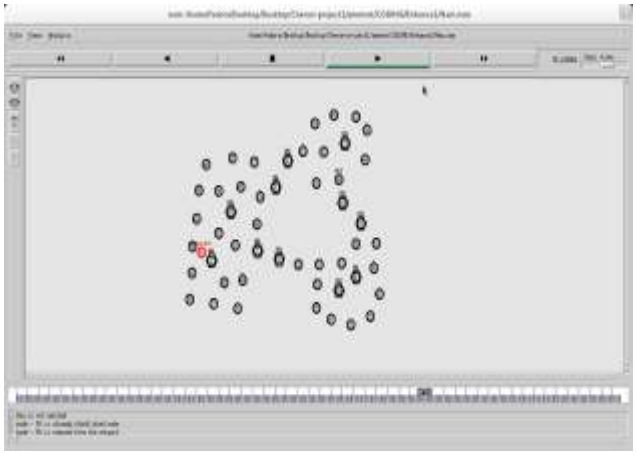

Fig.9. Attacker node

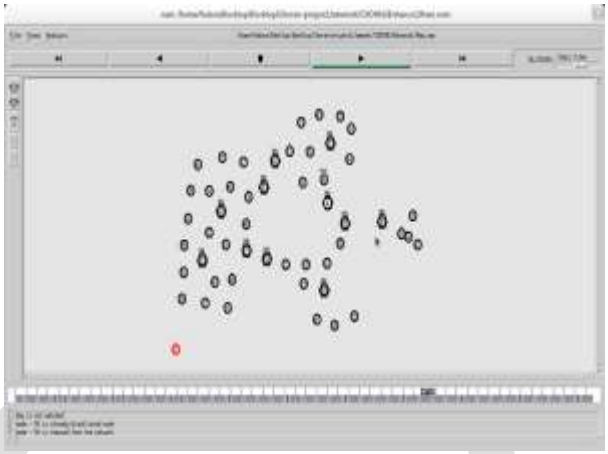

Fig.10. separate intruder node from network

CONCLUSION

Generally, the conventional mobile ad-hoc network suffer from network partitioning, this problem was solved in the AMMNET. It supports both intra-routing and inter-routing. Here, the mobile mesh routers of an AMMNET track the users and dynamically adapt the network topology and perform routing. It simply forwards the date from source to destination via multiple hops. This infrastructure provides full connectivity without need of high cost of network coverage.

This paper also describes a novel solution to the location tracking problem for mobile ad hoc networks. The estimated location for nodes is regarded as a probability distribution represented by a collection of sample points. The location information from the anchors is propagated through the network via local broadcasting of the location estimates. When a node receives the location estimates from neighbors, it updates its location distribution using the particle filtering method. And security can be provided by assigning separate key to all the nodes in the network, it can be done by group key management.

REFERENCES:

[1] Wei-Liang Shen, Chung-Shiuan Chen,Kate ChingJu Lin," Autonomous Mobile Mesh Networks",ieeetransactions on mobile computing,2014.

[2] G.S. Kasbekar, Y. Bejerano, and S. Sarkar, "Lifetime and Coverage Guarantees through Distributed Coordinate-Free Sensor Activation,"Proc. ACM MobiCom, 2009.

[3] Y. Bejerano, "Simple and Efficient k-Coverage Verification withoutLocation Information," Proc. IEEE INFOCOM, 2008.

[4] C.-F. Huang and Y.-C. Tseng, "The Coverage Problem in aWireless Sensor Network," Mobile Networks and Applications, 2005.

[5] X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C.Gill,"Integrated Coverage and Connectivity Configuration in Wireless sensor Networks," Proc. ACM First Int'l Conf. Embedded Networked Sensor Systems (SenSys), 2003.

[6] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," Wireless Comm. and Mobile Computing, 2002.

[7] p. Bahl, and V.N. Pamanbhan, "RADAR: An in-Building RF-Based User Location and Tracking System," Proceedings of the IEEE INFOCOM'00, March 2000.

[8] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low cost outdoor localization for very small devices," IEEE Personal Communications Magazine, vol. 7, no. 5, pp.28–24, October 2000.

[9] L. Girod and D. Estrin, "Robust Range Estimation using Acoustic and Multimodal Sensing," In Proceedings of IROS 01, Maui, Hawaii, October 2001.

[10] F. Kuhn, R.Wattenhofer, Y. Zhang, and A. Zollinger, "Geometric Ad Hoc Routing of Theory and Practice," PODC 2003, pp. 63-72, 2003.

[11] W.-H. Liao, Y.-C. Tseng, and J.-P. Sheu, ”GRID: A Fully Location-Aware Routing Protocol for Mobile Ad Hoc Networks,” Telecommunication Systems, vol. 18(1) pp. 37–60, 2001.

[12] W.-H. Liao, Y.-C. Tseng, K.-L. Lo, and J.-P. Sheu, ”Geogrid: A Geocasting Protocol for Mobile Ad Hoc Networks Based on Grid,” Journal of Internet Technology, vol. 1(2) pp. 23–32, 2000.

[13] C. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs", IEEE / ACM Transactions on Networking, vol. 8, no. 1,February 2000.

[14] M. Steiner, G. Tsudik and M. Waidner, “Key agreement in dynamic peer groups”, IEEE Transactions on Parallel and Distributed Systems, vol. 11,no. 8, pp.769-780, August 2000.