Hybridization of Routing and Tolerant Security Mechanism for WANET

Gavendra Sahu[1], Neelabh Sao[2]

[1]Rungta College of Engineering and Technology,
Kohka Kurud Road, Bhilai
gebu131184@gmail.com

[2]Rungta College of Engineering and Technology,
Kohka Kurud Road, Bhilai
neelabhsao@gmail.com

Abstract: ***Wireless Ad hoc Network is a network where there is no existence of wireless infrastructure for networking. Thus this kind of network have limited homogenous feature. In sensor networks, building efficient and scalable protocols is a very challenging task due to the limited resources and the high scale and dynamics uses the GRA (Geographic Routing Algorithm) to get this location information. With the availability of GRA, the mobile hosts knows there physical location. One main challenge in design of these networks is their vulnerability to security attacks. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. We use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of our security framework. In this paper main focus is on time, location, power control and security. In order to support time, location, power control and security of critical applications, we present DFSRTS, (Depth First Search Based Routing-Tolerant Security Mechanism).***

Keywords: DFS, GRA, greedy forwarding, LBK, ID based cryptography.

1. Introduction

Ad hoc networks consist of wireless hosts that communicate with each other in the absence of a fixed infrastructure. In recent years, ad hoc networks have gained a significant attention. In cases like disaster relief, conference, and battlefield environments, ad hoc networks are potentially applied. Sensor networks are a class of wireless ad hoc networks. Other contexts include rooftop networks, static networks with nodes placed on top of buildings, to be used when wired networks fail. In an ad hoc network, a message sent by a node reaches all its neighboring nodes that are located at distances up to the transmission radius. In case of multi hop wireless networks, the routes between nodes are normally created through several hops because of the limited transmission radius. Now-a-days unit graph model is accepted widely in many areas. In the unit graph model, two nodes, A and B, in the network are neighbors if the distance between them is utmost *R*, where *R* is the transmission radius that is equal for all nodes in the network. In case of face routing, a message is routed along the interior of the faces of the communication graph, with face changes at the edges crossing the S-D-line. The final routing path is shown in Fig.1.

Variations of this model include unit graphs with obstacles (or sub graphs of unit graphs), and manpower graphs where each node has its own transmission radius and links are allowed only when bidirectional communication is possible [7]. However, in power and cost savings and congestion-aware methods, in order to reach an intended receiver nodes may adjust their transmission power. In terms of reliability, the use of the nodes' position for routing poses evident problems. Considering the accuracy of the destination's position is an important problem. In some cases the destination is a fixed node (e.g., a monitoring center known to all nodes, or the geographic area monitored), and some networks are static. The problem of designing location update schemes to provide accurate destination information and enable efficient routing in mobile ad hoc networks appears to be more difficult than routing itself [8]. Using an optimal broadcasting scheme a message can be broadcast (i.e., flooded), if it is reasonably "short" [9].

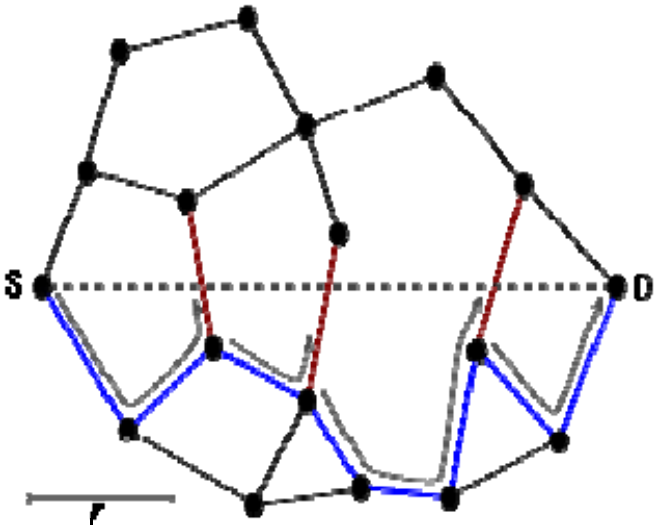

Figure 1: Unit graph representation of multi-hop wireless network

1.1 Geographic routing

Geographic routing (also called **geo routing** or **position-based routing**) is a routing principle that is based on geographic position information. This type of routing is mainly used for wireless networks. Instead of using the network address, it is based on the idea that the source sends a message to the geographic location of the destination. In 1980s, the idea of using position information for routing was first proposed in the area of packet radio network [11] and interconnection networks [12]. There are two things that are required by geographic routing. One is that each node can determine its own location and the other one is that the location of the destination should be known to the source. Without having knowledge of the network topology or a prior route discovery a message can be routed to the destination with the help of the above information. In each step using only local information, greedy forwarding tries to bring the message closer to the destination. Thus, each node forwards the message to the neighbor that is most suitable from a local point of view. The most suitable neighbor can be the one who minimizes the distance to the destination in each step by using greedy forwarding.

1.2 Immediate Pair wise Key Establishment

In order to establish pair wise shared keys between neighboring nodes link-layer security schemes demand an efficient method. Henceforth, such keys are referred to as immediate pair wise keys (or IPKs for short). Messages exchanged between neighboring nodes can be encrypted and authenticated with the help of IPKs, via efficient symmetric-key algorithms of two neighboring nodes. Adversaries, be they external or internal, may overhear the authentication messages, but cannot deduce the shared key for the lack of the LBKs [19] of node A and B. For different security purposes, Node A and B can derive various shared session keys by feeding messages into the hash function h. For example, they can use hash function for message encryption and for message authentication. In the similar way, each node can establish IPKs with all its legitimate neighbors after the neighbor discovery and authentication phase.

1.3 Multi-hop Pair wise Key Establishment

In addition to the IPKs, a node may need to establish pair wise shared keys with other nodes that are multi-hop away. We call such keys as multi-hop pair wise keys (or MPKs for short) that are required for securing end-to-end [15].

2. Related Work

Initially, the architectures for network survivability were proposed to improve both security and dependability of information systems in the Internet context [16], about the importance of all architectures to support the survivability concept, we high light SABER [17] and SITAR [18] architectures due to their completeness in terms of survivability properties as resistance, recognition, recovery and adaptation. Thus, SITAR coordinates all components and controls any request or response in a centralized or partially distributed way. The SABER architecture [17] integrates also different security mechanisms to improve the survivability of Internet services. Its multi-layer approach blocks, evades and reacts to a variety of attacks in an automated and coordinated way. SAMNAR [19], a Survivable Ad hoc and Mesh Network Architecture, whose goal is the design of survivable essential network services against attacks and intrusions. SAMNAR manages preventive, reactive and tolerant security mechanisms in an adaptive and coordinated way, focusing on the survivability of link-layer connectivity, routing and end-to-end communication. The location of nodes may be available directly by communicating with a satellite (for outdoor networks), using GPS (Global Positioning System), if nodes are equipped with a small low power GPS receiver. The position-based approach in routing becomes practical due to the rapidly developing software and hardware solutions for determining absolute or relative positions of nodes in indoor/outdoor ad hoc networks [10]. *Scalability* is sometimes judgmental and/or dependent on the performance evaluation outcome. A scalable solution is one that performs well in a large network. It has been experimentally confirmed [12] that routing protocols that do not use geographic location in the routing decisions, such as *AODV*, *DSDV*, or *DSR* (a recent survey is given in [13]) are not scalable. For instance, [12] describes GLS (scalable location service), similar to the doubling circle method independently proposed by Amouris, Papavassiliou, and Lu. Simple geographic forwarding [14] combined with *GLS* compares favorably with *DSR*; in large networks (over 200 nodes), it delivers more packets and consumes fewer network resources [12]. Similar conclusions were made in [11], where the depth-first search-based *GRA* scheme was compared with the *DSDV* protocol. Routing table sizes in *GRA* were logarithmic. Therefore, it is likely that only position- based approaches provide satisfactory performance for large networks.

3. Methodology

In this paper, we have tried to hybridize one or more security algorithm with one or more routing algorithm which can also be applied serially as well as parallel, in order to improve overheads of battery consumptions between any node that are either immediate neighbors or multi hop away. For security between two nodes we use the concept of location based keys (LBKs). Then, we design node to node neighborhood authentication which helps in achieving localizing the compromised nodes impact if any. Between any two nodes that are either immediate or multi hop away we establish pair wise shared keys such keys are fundamental keys are fundamental in providing security support for WANETs. Depending on the probabilities of nodes in the radio range, DFS use the same approach for each node between sources to destination. Based on this concept we propose the hybrid of routing and security mechanism for wireless ad hoc network known as DFSRTS.

3.1 Greedy Forwarding

Greedy forwarding (GF) is an efficient, localized ad hoc routing scheme employed in many existing geographic routing algorithms [1]. Under GF a node makes routing decisions only based on the locations of its (one-hop) neighbors, thereby avoiding the overhead of maintaining

global topology information. In each step a node forwards a packet to the neighbor with the shortest Euclidean distance to the destination [2]. An alternative greedy forwarding scheme [3] chooses the neighbor with the shortest projected distance to the destination on the straight line joining the current node and the destination.

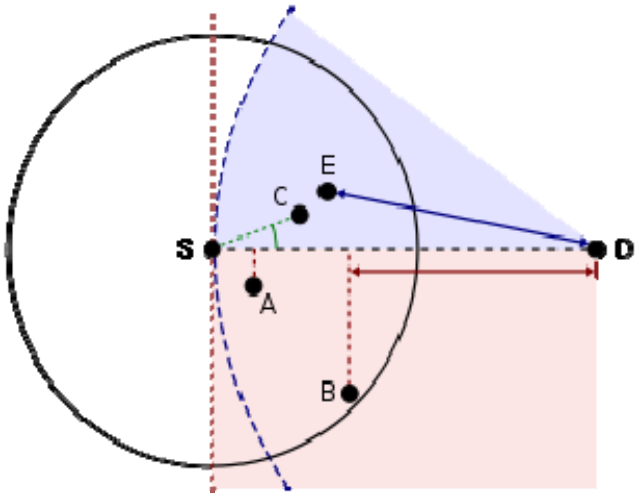

Figure 2: Greedy forwarding variants: The source node (S) has different choices to find a relay node for further forwarding a message to the destination (D). A = Nearest with Forwarding Progress (NFP), B = Most Forwarding progress within Radius (MFR), C = Compass Routing, E = Greedy

However, a routing node might encounter a routing void if it cannot find a neighbor that is closer (in term of Euclidean or projected distance) to the destination than itself. In such a case, the routing node must drop the packet or enter a more complex recovery mode [4] to route the packet around the routing void. In this section we prove GF always succeeds in sensing-covered networks when the double range property is satisfied.

3.2 Depth First Search

Geographic routing algorithm (GRA) requires nodes to partially store routes toward certain destinations (those for which they are concave) in routing tables [11]. GRA applies the greedy strategy in forwarding messages. If the information in routing tables is outdated, concave nodes start the route discovery protocol. The route discovery finds a path from S to D and updates the routing tables toward D at any node on the path with this information. After the route discovery protocol is successfully completed, the stuck packet can be routed from S to D. The authors propose two route discovery strategies: breadth first search (equivalent to flooding) and depth first search (DFS). DFS yields a single acyclic path from S to D. Each node puts its name and address on the route discovery packet *p*. Then it forwards *p* to a neighbor who has not seen *p* before. This neighbor is one of all the neighbors that minimize $d(S, y)+d(y, D)$, where $d(x, y)$ is the distance between nodes x and y. If a node has no possibilities to forward the packet, it removes its name and address from the packet and returns the packet to the node from which it originally received it. Route discovery packets are kept for some time. If a node receives the same packet twice, it refuses it. DFS can alternatively be used to deliver the packet without route discovery and routing tables, as independently proposed by the author of this tutorial (with applications for the construction of QoS paths).

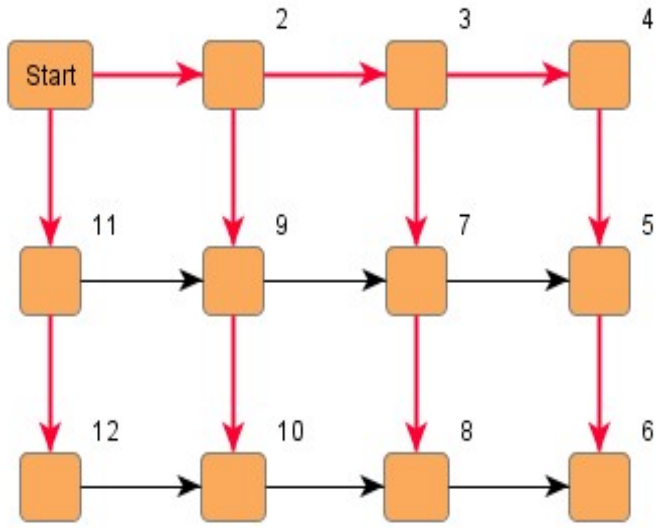

Figure 3: Depth First Search Traversal

3.3 Location-Based Key Management Scheme

Location-based key management scheme [20] for WANs, including the generation and distribution of LBKs, a secure LBK-based neighborhood authentication scheme, and 1) methods for establishing both immediate and multi-hop pair wise shared keys 2) Range-free localization. By contrast, the range-free localization approach does not rely on exact distance or range measurements. Instead, we assume that there are some special nodes called anchors knowing their own locations. All the non-anchor nodes autonomously derive their locations based on information from the anchors and neighboring nodes via secure range-free localization techniques.

3.4 Location-Based Neighborhood Authentication scheme

Neighborhood authentication is the process by which any two neighboring nodes validate each other's network membership [15]. This process is fundamental in supporting many security services in case of WANETs. For example, a node should only accept messages from and forward messages to authenticated neighbors. Otherwise, external adversaries can easily inject bogus broadcast messages into the network or swindle network secret information from legitimate nodes. In our scheme, new nodes can be added freely to maintain necessary network connectivity, especially when some existing nodes die out because of power shortage or other reasons. A new node is also required to execute the authentication protocol once localized properly.

4. Expected Outcome

It improves the performance of network and helps in creation of QoS path. This path satisfies delay and bandwidth criteria to improve the performance of network using location based

concept. Identity and location based immediate and multi hop pair wise keys provide tolerant security between nodes and end to end layer. DFS helps in finding feasible acyclic path from source to destination.

5. Advantages of this Approach

We proposed an efficient tolerant security mechanism to deal with routing, security, power management, bandwidth management, mobility management, etc. The proposed approach uses DFS, GREEDY algorithm in a Multi hop network. This work presents tolerant security mechanism architecture for ad hoc and mesh networks called DFSRTS. DFS provides the most feasible route for message transmission which consumes less battery of the node having unable to find nodes within the radio range of node by greedy approach. This model provide more security by using the concept of cryptography which uses key management scheme and helps in proper management when there is any change in location of nodes by using GRA.

6. Conclusion and Future Work

In this paper, first we apply geographic routing to find the nearest neighbor of the source node within the radio range after that cryptographic network neighborhood approach is applied between intermediate and then depth first search approach is applied to find efficient route between source and destination. Its goal lies in making these networks able to provide essential services even in face of attacks and intrusions. DFSRTS is based on a coordinated integration among the preventive, reactive and tolerant defense lines, being able to self-adapt to different network conditions. Results point out that our approach significantly decreases the impact of routing attacks with minimal performance loss.

References

[1] G. Finn. Routing and addressing problems in large metropolitan-scale internetworks. Technical Report ISI Research Report ISU/RR-87-180, Inst. for Scientific Information, Mar, 1987.

[2] B. Karp and H. T. Kung. Gpsr: greedy perimeter stateless routing for wireless networks. In Proceedings of the 6th annual international conference on Mobile computing and networking, pages 243{254, 2000.

[3] H. Takagi and L. Kleinrock. Optimal transmission ranges for randomly distributed packet radio terminals. IEEE Transactions on Communications, 32(3):246{257, 1984.

[4] L. Chen and C. Kudla, .Identity based authenticated key agreement protocols from pairings, Cryptology ePrint Archive, Report 2002/184, 2002.

[5] Takagi, H.; Kleinrock, L. (March 1984). "Optimal transmission ranges for randomly distributed packet radio terminals". *IEEE Transactions on Communications* 32 (3): 246–257.

[6] Finn, Gregory G. (March 1987). Routing and Addressing Problems in Large Metropolitan-Scale Internetworks. University of Southern California, ISI/RR-87-180.

[7] L. Barriere *et al.*, "Robust Position Based Routing in Wireless Ad Hoc Networks with Unstable Transmission Ranges," *Proc. 5th ACM Int'l. Wksp. Discrete Algorithms* July 2002, 2001, pp. 19–27.

a. Stojmenovic, "Location Updates for Efficient Routing in Ad Hoc Networks," *Handbook of Wireless Networks and Mobile Computing*, Wiley, 2002.

[8] Stojmenovic, M. Seddigh, and J. Zunic, "Dominating Sets and Neighbor Elimination Based Broadcasting Algorithms in Wireless Networks," *IEEE Trans. Parallel Dist. Sys.*, vol. 13, no. 1, Jan. 2002, pp. 14–25.

[9] J. Hightower and G. Borriello, "Location Systems for Ubiquitous Computing," *IEEE Comp.*, Aug. 2001, pp. 57–66.

[10] R. Jain, A. Puri, and R. Sengupta, "Geographical Routing Using Partial Information for Wireless Ad Hoc Networks," *IEEE Pers. Commun.*, Feb. 2001, pp. 48–57.

[11] J. Li et al., "A Scalable Location Service for Geographic Ad Hoc Routing," *Proc. ACM MOBICOM 2000*, pp. 120–30.

[12] Y.C. Tseng, W.H. Liao, and S.L. Wu, "Mobile Ad Hoc Networks and Routing Protocols," *Handbook of Wireless Networks and Mobile Computing*, I. Stojmenovic, Ed., Wiley, 2002, pp. 371–92.

[13] G. G. Finn, "Routing and Addressing Problems in Large Metropolitan-Scale Internetworks," ISI res. rep. ISU/RR-87-180, Mar. 1987.

[14] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks," *IEEE Comp.*, Vol 24, no.2, feb. 2006, pp. 1–14.

[15] K. John, C. Dennis, H. Alexander, W. Antonio, C. Jonathan, H. Premkumar, and D. Michael, "The willow architecture: comprehensive survivability for large-scale distributed applications," in *2002 DSN*.

i. Keromytis, J. Parekh, P. N. Gross, G. Kaiser, V. Misra, J. Nieh, D. Rubenstein, and S. Stolfo, "A holistic approach to service survivability," in *Proc. 2003 ACM SSRS*, pp. 11–22.

[16] F. Wang and R. Upppalli, "SITAR: a scalable intrusion-tolerant architecture for distributed services," in *Proc. 2003 DISCEX*, vol. 2, pp. 153–155.

[17] Michele Nogueira, Helber Silva, Aldri Santos, and Guy Pujolle, "A Security Management Architecture for Supporting Routing Services on WANETs," *IEEE, Trans.on network and service mgmt*, vol 9, no.2, june. 2012, pp.156–168.

[18] Yong Ho Kim, Jong Hwan Park, Dong Hoon Lee and Jongin Lim "Bogus data Filtering in sensor networks" Center for Information Security Technologies (CIST), Korea University, Seoul, Korea {*f*optim, decartian, donghlee, jilim*g*@korea.ac.kr}

Author Profile

Gavendra Kumar Sahu received the B.E. degree in Computer Science Engineering from Raipur Institute of Technology and Engineering, Raipur, in 2006, and pursuing M.Tech. in Software Engineering from Rungta College of Engineering and Technology, Bhilai, in 2011. His current research interest is to model tolerant security mechanism using DFS and GRA algorithm to reduce the energy consumption in WANET.

Neelabh Sao received B.E from Rungta College of Engineering and Technology, Bhilai, India, in the year 2003 and later did his M.Tech in CSE from Rungta College of Engineering and Technology, Bhilai, India. Currently he is working as an Assistant Professor in Rungta College of Engineering & Technology (Department of Computer Science and Engineering), Bhilai, India. His area of interest includes Data Mining.