Security Enhanced Dynamic Routing Algorithm for Wireless Sensor Network

Ms. Nidhi Bansod
M.Tech 4th Sem
PIET, Nagpur

Abstract:
In this project we deal fully about the security which has become one of the major issues for data communication for wired and wireless networks. Different from the past work on the designs of cryptography and system infrastructure, a dynamic routing algorithm is proposed that could randomize delivery paths for data transmission. The algorithm is easy to implement and compatible with popular routing protocols, such as Routing Information protocol in wired networks and Destination sequenced distance vector protocol in wireless networks, without introducing extra control messages. An analytic study on the proposed algorithm is presented, and a series of simulation experiments are conducted to verify the analytic results and to show the capability of proposed algorithm. In the past decades, various security-enhanced measures have been proposed to improve the security of data transmission over public networks. Existing work on data transmission includes the designs of cryptography algorithms and system infrastructures and security enhanced routing methods. The main objective of the project is to propose a dynamic routing algorithm to improve the security of data transmission.

Keywords- Cryptography algorithms, Destination Sequenced Distance Vector routing protocol,security.

1.Introduction

Various security enhanced measures have been proposed to improve the security of data transmission over public data networks. Existing work on security enhanced data transmission includes the designs of cryptography algorithms and system infrastructures and security enhanced routing. Their common objectives are often to defeat various threats over the Internet, including eavesdropping, spoofing, hijacking etc. Among many well known designs for cryptography based systems, the IP security (IPSec) [23] and the secure socket layer (SSL) [21] are popularly supported and implemented in many systems and platforms. Although IPSec and SSL greatly improve the security level for data transmission, they unavoidably introduce substantial overheads [1], [7], [13], especially on gateway host and effective network bandwidth. For example the data transmission overhead is 5 cycles/byte over an intel pentium II with the Linux IP stack alone and the overhead increases to 58 cycles/byte when Advanced Encryption Standard (AES) [10] is adopted for encryption/decryption for IPSec. Another alternative for security enhanced data transmission is to dynamically route packets between each source and its destination so that the chance for system break-in, due to successful interception of consecutive packets for a session. Intension of security enhanced routing is different from adopting paths between a source and a destination to increase the throughput of data transmission.

2. Table driven scheme

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad-hoc mobile network based on the Bellmen-Ford algorithm. It was developed by C.Perkins and P.Bhagwat in 1994. The main contribution of the algorithm was to solve the Routing Loop problem. Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an old no is used. The no is generated by a destination, and the emitter needs to send out the next update with this no. Routing information is distributed between nodes.

Selection of Route

If a router receives new information, then it updates the latest sequence no. If the sequence no is the same as the one in the routing table then the route with better metric is used. Stale entries are those entries that have not been updated for a while. Such entries as well as the routes using those nodes as next hops are deleted.

3. Position based hybrid routing algorithm

The proposed algorithm PBHRA comes under position based algorithm class in hybrid main category. In the proposed algorithm the central node, in other words a master node is assigned as it directs the routing information in infrastructure wireless networks. When nodes are required to send data to a target node, they take the location of target node and the route to achieve it from master node. Accordingly they send their data through that route. At this stage, the proposed algorithm differs from infrastructure wireless networks since data is sent via central station in infrastructure wireless networks. However in proposed algorithm, the master node which behaves as if it is the central node helps only while finding the route to achieve the target.

3.1 Destination sequenced distance vector (DSDV) protocol

This routing method allows a collection of mobile computers, which may not be close to any base station and can exchange data along changing arbitrary paths of

interconnection, to afford all computers according to their numbers a (possibly multi-hop) path along which data can be exchanged. In addition our solution must remain compatible with operation in case where a base station is available. Packets are transmitted between the stations of the network by using routing tables which are stored at each station of the network. Each routing table at each of the stations lists all available destinations and the no of hops to each.

4. Security Goals:

In the ideal world, a secure routing protocol should, guarantee the integrity and authenticity, and availability of messages availability in the presence of adversaries of arbitrary power. Every eligible receiver should receive all messages intended for it and be able to verify the integrity of every message as well as the identity of sender.

In our view, protection against eavesdropping is not an explicit security goal of a secure routing algorithm. Secrecy is the most relevant to application data, and it is not the responsibility of a routing protocol to provide it. However, we do consider it the responsibility of a routing protocol to prevent eavesdropping caused by misuse of the protocol itself. Eavesdropping caused by the rerouting of a data flow should be prevented.

Similarly, we believe protection against the replay of data packets should not be a security goal of a secure routing protocol. This functionality is best provided at the application layer because only the application can accurately detect the replay of data packet (for example as opposed to retransmissions). In the presence of outsider adversaries, it is conceivable to achieve this idealized goals. However, in the presence of compromised or insider attackers, especially those with laptopclass capabilities, it is most likely that some if not all of this goals are not fully achievable. Rather, instead of complete compromise of the entire network,the best we can hope for in the presence of insider adversaries is graceful degradation.

4.1 Adaptive Routing:

Adaptive routing describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaption is intended to allow as many routes as possible to remain valid (that is to have destination that can be reached) in response to the change. People using a transport system can display adaptive routing. For example if a local railway station is closed, people can alight from a train at a different station and use another method, such as a bus to reach their destination. The term is commonly used in data networking to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes so long as other path choices are available. There are several protocols used to achieve this:

1. RIP
2. OSPF
3. IS-IS
4. IGRP/EIGRP

4.2 Properties of DSDV protocol:

The DSDV protocol guarantees loop free paths to each destination. To see why this property holds, consider a collection of IV mobile hosts forming an instance of an ad-hoc style network. Further assume that the system is in steady state, i.e. routing tables of all nodes have already converged to the actual shortest paths. At this instant, the next node indicators to each destination induce a tree rooted at that destination. Thus , routing tables of all nodes in the network can be collectively visualized as forming IV trees, one rooted at each destination. In the following discussion, we'll focus our attention on one specific distance x and follow the changes occurring on the directed graph G(a) defined by nodes I and arcs (i, p;) where p: denotes the next-hop for destination x at node i. Operation of DSDV algorithm ensures that at every instant G(z) is loop-free, or rather, it is a set of disjoint directed trees directed. Each such tree is rooted either at z or at a node whose next-hop is nil. Since this property holds with respect to each destination z, all paths induced by routing tables of DSDV algorithm are indeed loop free at all instants.

Potentially a loop may form each time node i changes its next hop. This can happen in two cases. First, when node i detects that the link to the next hop is broken, the node resets p_i to nil. This action cannot form a loop involving i. The second scenario occurs when node i receives from one of its neighbors, a route to z, with sequence number s_k and metric m is selected to replace the current route it has through p_i. Let s_i denote the value of the sequence number stored at node i and di denote the distance estimate from i to z just prior to receiving route from k. i will change its next hop from p_i to k only if either of the following two happens.

1. The new route contains a newer sequence number i.e. $s_k > s_i$.
2. The sequence number s_k is same as s_i but the new route offers a shorter path to x i.e. $m<d_i$.

Results :

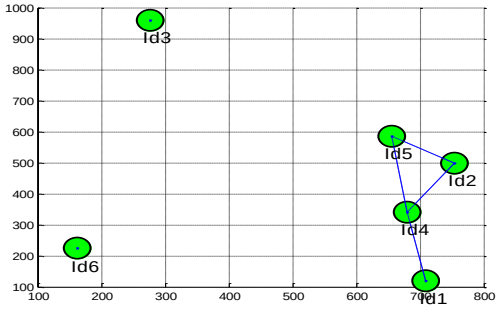

Fig. communication between nodes

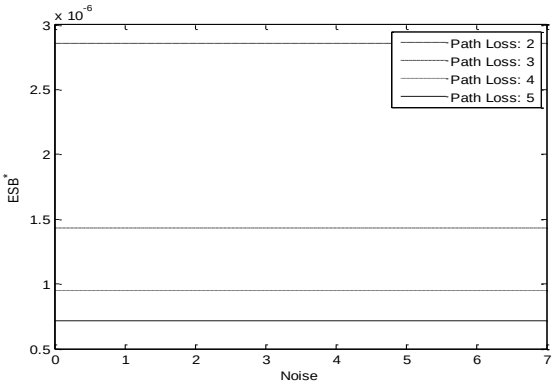

Fig. Reduced path loss

Conclusion

In this study the proposed PBHRA algorithm is compared with table driven, on demand and position based algorithms in terms of normalized routing load, packet delivery fraction and end to end packet delay. It was observed from performance values that the PBHRA gives better results than table driven, on demand and position based algorithms especially in the case of high mobility. The PBHRA algorithm uses available bandwidth efficiently because of its high packet delivery fraction and low normalized routing overload. The algorithm is not affected with the number of nodes increased in the network. Further security can be achieved by reducing the time delay, path losses and collisions due to irregular acknowledgments.

References

[1] Abolhasan M, Wyosocki T, Dutkiewicz E (2004). A review of routing protocols for mobile *ad hoc* networks. *ad hoc* networks 1: 1-22.

[2]. Basagni S, Chiamtac I, Syrotiuk VR, Woodward BA (1998). A Distance Routing Effect Algorithm for Mobility (DREAM),Proceedings of the 4th International Conference on Mobile Computing and Networking pp. 76-84.

[3]. Corson S, Macker J (1999). Mobile Ad hoc Networking (MANET):Routing Protocol PerformanceIssuesandEvaluationConsiderations.IETF ;http://www.ietf.org/rfc/rfc2501.txt.

[4] Demirci R (2007). Similarity relation matrix-based color edge detection. Int. J. Elect. Commun. (AEU), 61: 469-478.

[5] Ehsan H, Uzmi ZA (2004). Performance Comparison Of *Ad Hoc* Wireless Network Routing Protocols. INMIC 2004; 0-7803-8680-IEEE.

[6] Hwang S, Chien C, Wang C (2005). A Novel GPS-Based Quorum Hybrid Routing Algorithm (GPS-QHRA) for Cellular-Based *Ad Hoc* Wireless Networks. J. Inform. Sci. Eng. pp. 1-21.

[7] Joe I, Batseli SG (2002). MPR-Based Hybrid Routing for Mobile Ad-Hoc Networks. Proceedings of the 27th Annual Conference on Local Computer Networks (LCN'02) IEEE Computer Society pp.7-12.

[8] Lin X (1999). GPS based localized routing algorithms for wireless Networks. Bsc Thesis. Ottawa-Carleton Institute for Computer Science School of Information Technology and Engineering pp. 25-29.

[9]. Perkins CE, Royer EM (1999). Ad-Hoc on Demand Distance Vector Routing. Proc. Of 2nd IEEE Wksp. Mobile Comput. Applic. pp. 90-100.

[10] Stajmenovic I (2002). Position Based Routing in *Ad Hoc* Networks.IEEE Commun. Magazine 7: 128-134.

[11] Watanabe M, Higaki H (2007). No-Beacon GEDIR: Location-Based Ad-Hoc Routing with Less Communication Overhead.International Conference on Information Technology (ITNG'07).

[12]. Wattenhofer R (2005). Algorithms for *ad hoc* and sensor Networks. Comp. Commun. 13: 1498-1504.

[13]. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[14] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, System architecture directions for networked sensors," in *Proceedings of ACM ASPLOS IX*, November 2000.