SECURE ROUTING IN WIRELESS SENSOR NETWORKS: ROUTING PROTOCOLS

[1]A.Senthilkumar and [2]Dr.C.Chandrasekar

[1]Assistant .Professor, Department of MCA,
Sengunthar Engineering College, Tiruchengode - 637205, Tamilnadu, India.
senthilkumarmca76@gmail.com
[2]Associate Professor, Department of Computer Science,
Periyar University, Salem - 636011, Tamilnadu, India.
ccsekar@gmail.com

Abstract

A Secure Routing capabilities on the order of Node to Base Station will be capable of both wired connectivity to the internet as well as wireless connectivity to the sensor network. One aspects of sensor networks organized hierarchically, with a base station serving as a gateway for collecting data from a multi-hop network of resource-constrained sensor nodes. Strategies for multiple destination base stations is analyzed as a strategy to provide tolerance against individual base station attacks and or compromise. Test performance should be similar to Optimization Methods.

Keywords: Wireless Sensor Networks, Energy aware Routing, Resource Constraint Sensor Nodes, Sensor Network Architecture, Secure Routing, Protocols, Base Station Placement.

I .INTRODUCTION:

Wireless sensor networks growing in popularity of application and wide range of application are emerging location aware sensor networks in the office and home. A notable feature of the architecture of a wireless sensor network is its hierarchy, rooted in a base station. One aspects of Sensor networks that complicates the design protocol aggregation work in secure routing. End-to-end security is possible in more conventional networks because the intermediate routers to have access to the content of messages. Proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes. We consider strategies for securing the sensor network, multipath routing to multiple destination base stations is analyzed as a strategy to provide tolerance against individual base station attacks. This strategy is considered both for the route discovery phase and data routing phase. Confusion of address and field identification in header and function. The relocation of base station in the network topology our analyze the extent to which base station mobility and placement can affect the network. The test performance of the three strategies, we have simulated wireless sensor networks in ns2 simulator.

1.1 Node to Base Station (BS) Secure Routing :

Sensor nodes use Kn to encrypt and transmit the data. Transmission of encrypted data from nodes to cluster leader. Appending id# to data and then forwarding it to higher level of cluster leaders, eventually reaching the base station.

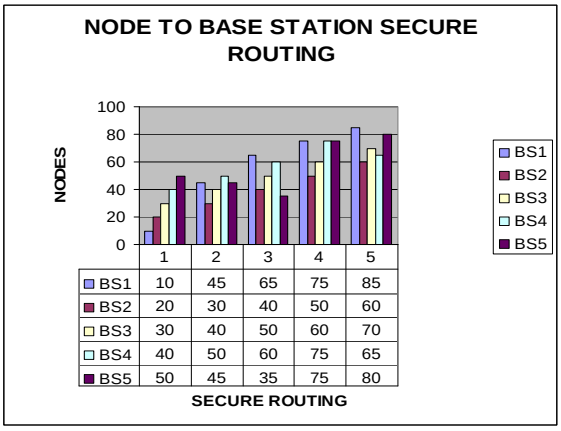

Figure1: Node to Base Station Secure Routing.

1.2 Nodes to Base Station (BS) Secure Routing Algorithm:

Step 1: if sensor node i want to send data to its cluster leader go to step 2, else exit the algorithm. Step 2: Sensor node i requests the cluster leader to send the Kc to decrypt the data if needed. Step 3: Sensor node i uses Kc and its own Kn to computer the encryption key Ki, Cn. Step 4: Sensor node I encrypts the data with Ki, Cn and appends its ID# and the Ts to the encrypted data and then sends them to the cluster leader. Five Main Contribution We purpose threat models and security goals for secure routing in wireless sensor networks. (i) Multiple base stations: Route Discovery, Route Request, Route feedback, Performance Evaluation of Route Discovery. (ii) Multiple Base Stations: Performance Evaluation of Multiple Paths, Passive Attack by Compromised

Sensor Nodes, Base Station Failure, Base Station Scalability. (iii) Disguising Base Station Location: Confusion of ID's, Relocation of Base Stations. (iv) Base Station Placement Strategies: Possibility of Relocating Base Stations, Determining Optimal Locations. (v) Attacks on Sensor Network Routing: Selective Forwarding, Attack on Specific Sensor Network Protocols.

II. TEST THE PERFORMANCE OF THE THREE STRATEGIES AND ALGORITHMS CAN BE USED FOR THE DESIGN:

We have simulated wireless sensor networks in ns2 Simulator, for a Random Network Topology we generate 100 Nodes and put them in a 1250 * 1250 M^2 Square Area. For Grid Network Topology, we generate 7 * 7 Nodes and put them in a 1430 * 1430 M^2 Square Area. For each Experiment, we randomly generate 15 to 25 Network Topologies. The results shown in various graphs in the paper are average values of each test. Small (<10 Network devices) Medium (~ 25 devices) Wireless access networks, such as CDMA based and fixed wireless (WLL) networks.

2.1Objectives that motivated the Development of the new Heuristic Design Methods:

The methods should be capable of designing efficient medium and large- scale access networks at polynomial time. Their performance should be similar to that of other optimization methods, as for instance the ones presented.

2.2.1 Performance of Study Large Networks:

Moreover their performance usually degrades quickly with the number of nodes (because a unique resource has to be shared among all) we will thus abstract from the MAC layer and focus on routing protocols. This will enable us to study large networks and propose simpler, more tractable mathematical models, more suitable for computer simulations.

2.2.2 Various energy-aware Routing Protocols and Two Broad Categories:

We will study various energy-aware routing protocols, propose different data traffic patterns and network sizes and we will study how well the different protocols scale with the number of node and if differences in generated network structures appear. Routing protocols for sensor networks are divided in two broad categories: Pro-Active Protocol, Reactive (or on-demand) Protocols.

2.2.3 Protocols belonging and enables a Node:

The protocols belonging to the first group to build a network image locally at each node, this enables a node to quickly determine a route to any destination when it has a packet to route. The major problem with this approach is that it requires a lot of control traffic to propagate all the necessary network information to all the nodes and this image must then be regularly updated, this being also a cause of network traffic.

2.2.4 Two kinds of data traffic will be simulated: The first one is converge casting, where all nodes send data to one or more sinks (data collection points). It is a typically data collection scenario. The second one is random unicast (one to one) communications between nodes, and is less focused on an application. To simplify mathematic modeling, we will restrict the study to static networks, and won't include mobility. Network size will vary between tens to hundreds of nodes. Most traffic in Sensor Networks can be classified into one of three Categories: Many-to-Many: Multiple Sensor Nodes send sensor reading to a base station or aggregation point in the network. One-to-Many: A Single node (typically a base station) multicasts or floods a query or control information to several sensor nodes. Local Communication: Neighboring nodes send localized messages to discover and coordinate with each other. A node may broadcast messages intended to be received by all neighboring nodes or unicats messages intended for a only single neighbor.

III. EFFICIENT SOLUTION FOR WIRELESS COMMUNICATION SYSTEMS:

Recent years have witness tremendous developments regarding wireless network access. Given to methods for the design of in-door coded division multiple access (CDMA) based wireless networks and fixed wireless (e.g. wireless local loop- WLL) networks, which are referred to as wireless access networks, In these networks.

3.1 Two main types of Network Components:

3.1.1 The Access Point / Base and Fixed Wireless User / Terminal Station:

Each terminal should be connected to only one access point / base station and each access point / base station together with its associated terminals, constitute an access subnetwork. Moreover, the access point / base stations can be connected to one or more other subnetworks (e.g. the backbone subnetwork). The fixed wireless terminals (test points) claim for access to the network and the access point / base stations connect the terminals to the network. With the set T of fixed wireless terminals and the set S of possible (predefined) locations for the placement of access point / base stations.

3.2 The Process of wireless Network Planning Basically Consists of Three Phases:

3.2.1 Base Station Placement and Wireless Terminal (test point) Empirical Approaches:

A number of base stations must be placed in a number of (predefined candidate sites, essentially one base station in each selected sites. The design cost that have refers to base station placement

(installation) and operation, should be minimum unfortunately, today there are no systematic methods to address the problem of wireless network planning, especially for CDMA based networks, fixed wireless and UMTS access networks. Allocation to the selected base station(s) in phase 1.practically, both phases can be considered as one. The planning process is mainly based on empirical approaches, nevertheless, recent design approaches based on integer linear programming (ILP) and mixed integer programming (MIP) techniques, deal with the above problem in a rather interesting way that it may be very advantages in practice. Integer Linear Programming (ILP): A wireless system planning procedure for in-door CDMA networks based on a complex Integer Linear Programming. Mixed Integer Programming: Simulation results regarding topologies with more that 27 wireless users are provided. In a series of complex MIP optimization models specially suited for UMTS base station planning are presented. The optimization methods are time demanding when applied to the solution of the design problems they involve particularly when the number of the network devices increase.

IV. WIRELESS LAN DATA SERVICES:

Wireless LAN data services provide moderate data rate and wide coverage area access to packets-switched data networks. The data networks emerged after the success of the paging industry to provide a two-way connection for larger messages. WLANs provide high data rates (maximum of iMbps) in a local area (< 100m) to provide access to wired LANs and the Internet. Today all successful WLANs Operate in unlicensed bands that are free of charge and rigorous regulations.

4.1 Penetration of Signals:

If one intends of bring a wireless service to the rooftop of a residence and distribute that service inside the house using other alternative such as existing cable or TP wiring that person may select LMDS equipment operating in licensed bands at several tens of GHz. If the intension is to penetrate the signal into the building for direct wireless connection to a computer terminal, the person may prefer equipment operating in the unlicensed ISM bands at 900 MHz or 2.4 GHz. The first approach is more expensive because it operates at licensed higher frequencies, where implementation and the electronics are more expensive and the frequency bands. The second solution does not have any interference control mechanism because it operates in unlicensed bands.

4.2 Packet Size in Wireless Data Networks Access Methods for Wireless LANs:

Problem 1: Determine the transfer time of a 20 KB file with a Mobile Data Network with a Transmission rate of 10 Kbps.

Solution : the early mobile data networks, such as ARDIS and mobile, limited the length of a file to around 20KB for a data rate of around 10Kbps it would take 20 (KB) * 8 (B / b) * 10 Mbps = 16 Seconds to transfer such a file.

Problem 2: Repeat for an 802.11 WLAN operating at 2 Mbps.

Solution: An IEEE 802.11 Network Operating at 2 Mbps should Transfer this file in 80ms.

Problem 3: What is the length of the file that the WLAN of Part (b) can carry in the time that mobile data service of part (a) carries its 20KB file.

Solution: In a 16 –Second time interval the same WLAN transfers a 4MB file.

V. ROUTE FEEDBACK

Each sensor node sends its local connectivity information (a set of identities of its neighbor nodes as well as the path to itself from A base station B) back to the base station B using A feedback message. A separate feedback message is send to every base station whose request message was forwarded in the first round. The mechanism used to send feedback messages to different base stations is same. After a node has forwarded its request message in round one. It waits a certain timeout interval before generating a feedback message. This interval allows a node to listen to the local broadcasts of its neighbors, who will also be forwarding the same request message. A feedback message containing neighbor list and path to B is propagated to B using the reverse path taken the request message initiated by B.

5.1 Four Different Computing Scenarios could be adopted

Two independent routes available between every node and one of the base stations, our protocol's goal is to route messages correctly in the presence of a single node. Protocol deals quite well with multiple nodes as well. We have performed a set of experiments to measure the number of nodes that can be blocked when a set of nodes turn and (simply) drop data packets. The average number of nodes that can be blocked as a function of the number of nodes. A single base station with a single path. A single base stations with two redundant paths. Three base stations with a single path. And Three base stations with two redundant paths (computed using the second strategy).

5.2 Attacks are difficult to address completely at the network level

These attacks must be addressed at multiple levels in our analysis, we have assumed that sensor nodes use an appropriate rate-based control mechanism while forwarding data packets, but not other nodes. However, a node in the vicinity of a base station can isolate that base station from the rest of the network by simply launching.

5.3 Launching experiments with two topologies are tested

In random generates topology; the position of each node is randomly selected. While in the grid topology, each node is placed on a square grid to accommodate the simulator, it was necessary to per tub each position in grid topology to a small region around each vertex in a square grid graph.

5.4 Attack Compromised by Active Sensor Node

Performed a set of experiments to analyze the effect of an active attack. The attack we have simulated in these experiments is comprised of repeatedly, sending data packets to the base stations to block the wireless medium and not allow other nodes to send their data packets.

5.5 A key management of probabilistic approach towards multiple base Stations

A key of deploying multiple base stations in a wireless sensor network can tolerate failure of one or more base stations. Number of sensor nodes that cannot reach any base station as a result of one or more base station failure. Four different computing scenarios, comprising of two, three, four, and five base stations respectively. In all computing scenarios, two redundant paths were computed using the second strategy. Base station failures automatically to relate by having redundant base stations.

VI. CONCLUSION & FUTURE WORK

Secure routing is acceptance and use of sensor networks for many applications. Base station is analyzed as a strategy to provide individual base station attacks or sensor node compromises problem to design a sensor network routing protocol that satisfies our proposed security goals. The possible presence of laptop-class adversaries and insiders and the limited applicability of end-to-end security mechanisms careful protocol design as well.

- Applications for wireless sensor networks.
- Characteristics of wireless sensor networks.
- Efficient heuristic solutions for wireless communication systems.
- Requirements for routing algorithms.
- Algorithms and protocols for wireless sensor networks.
- Traditional mechanisms.
- Data-driven mechanism.
- Performance evaluation of Route discovery and multiple path.
- Confusion of ID's.
- Wireless LAN data services.
- Wireless Network Process.

VII. REFERENCES

1 Guanqun Yang and Daji Qiao, "Barrier Information Coverage with Wireless Sensors", In Proc. IEEE INFOCOM 2009.

2.D.Ganesan, R.Govindan,S.Shenker and Estrin "Energy Efficient Multipath Routing in Wireless Sensor Networks" Mobile Computing and Communication Review,Vol 1,2008.

3. Muhammad Mahmudul Islam, Ronald Pose and Carlo Kopp, (2008).Routing Protocols for Adhoc Networks.

4. Dormido, S.; Sánchez, J.; Kofman, E. Sampling, event-based control and communication (in Spanish). *Rev. Iber. Auto. Infor. Indu.* 2008, *5*, 5–26.

5.Guanqun Yang, Wei Zhou and Daji Qiao, "Defending Against Barrier Intrusions Using Mobile Sensors" In Proc. International Conf. on Wireless Algorithms, Systems and Applications, 2007.

6.Prof.Dr.Gunnar Karlsson KTH Stockholm, Wireless Content Distribution, 2006

7.Srdan Capkun, Jean-Pierre Hubaux, Secure positioning of wireless devices with application to sensor networks. IEEE INFOCOM, March 2005.

8.Bryan Parno, Adrian Perrig and Virgil Gligor. Disotributed Detection of Node Replication Attacks in Sensor Networks. IEEE Symposium on Security and Privacy 2005.

9.Wensheng Zhang, Guohong Cao, Group Releying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-Based Approach. IEEE INFOCOM, March 2005.

10.A.A. Somasundara, A.Ramamoorthy, and M.B.Srivastava. Mobile Element Scheduling for Efficient Data Collection in Wireless Sensor Networks with Dyanmic Deadlines, 2004.

11. Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen and Pramod Varchney. A Key Management Scheme for Wireless Sensor Networks Using Depolyment Knowledge. IEEE INFOCOM'04, March 7—1,2004, HongKong.

12. C. Karlof and D.Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003

13.J.Deng, R.Han and S.Mishar, "The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks", to appear in IEEE 2nd International Workshop on Information Processing in Sensor Networks(IPSN '03), Palo Alto, CA, USA, April,2003.

14. C.Karlof and D.Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

15. Wood, J.A. Stankovic. "Denial of Service in Sensor Networks." IEEE Computer, 35(10): 54-62, October 2002.

A.Senthilkumar received the MCA Degree from the Madras University, India, in 1999. He received the M.Phil degree in Computer Science, Manonmaniam Sundharnar University, Tirunelveli, India. He is Currently Assistant Professor in Department of MCA, Sengunthar Engineering College, Tiruchengode, India. He has 11 Years of Experience in Teaching. And Currently Pursuing PhD degree in computer applications from Anna University Coimbatore, India. His fields of interest, Computer Networks, Network Security, Wireless Sensor Networks. He Has 12 Publications to his credit in National, and International Journals and Conference.

Dr.C.Chandrasekar received the PhD Degree from the Periyar University, Salem, India. He is Currently Associate Professor in Department of Computer Science, Periyar University, Salem, India. He has 14 Years and 3 Months of Experience in Teaching. His fields of interests Mobile and Communication Networks. He Has 32 Publications to his credit in National, International Journals and Conference.