ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

Preventing Attacks from Eavesdropper Using HMAC Protocol in Wireless Sensor Networks

Boopathy.S[1] Jayanthi.K[2]

PG Scholar, Department of ECE, SNS College of Technology, Coimbatore,India[1]

Associate Professor, Department of ECE, SNS College of Technology, Coimbatore,India[2]

Abstract-A wireless sensor network (WSN) is composed of numerous small sensing devices with limited communication range. The sensors collect data from the environment and report them to the sinks. With the promising sensing and wireless technologies, sensor networks are expected to be widely deployed in a broad spectrum of civil and military applications. Location information of the sinks, the sensors, and the objects being tracked are very important in sensor networks. Protecting location privacy in sensor networks is crucial considering different kinds of attacks that may disrupt the normal function of the networks. To identify location privacy issues in sensor networks and computes lower bound on the communication overhead to resolve those issues in order to achieve higher level of privacy. The two techniques to provide location privacy to monitored objects (source-location privacy)—periodic collection and source simulation—and two techniques to provide location privacy to data sinks (sink-location privacy)—sink simulation and backbone flooding. These techniques provide trade-offs between privacy, communication cost, and latency. Through analysis and simulation, we demonstrate that the proposed techniques are efficient and effective for source and sink-location privacy in sensor networks.

Keywords-Sensor networks, Network security, location privacy, source simulation, sink simulation.

I. INTRODUCTION

Sensor networks have been envisioned to be very useful for a broad spectrum of emerging civil and military applications. However, sensor networks are also confronted with many security threats such as node compromise, routing disruption and false data injection, because they normally operate in unattended, harsh or hostile environment. For applications like military surveillance, adversaries have strong incentives to eavesdrop on network traffic to obtain valuable intelligence. Abuse of such information can cause monetary losses or endanger human lives. To protect such information, researchers in sensor network security have focused considerable effort on finding ways to provide classic security services such as confidentiality, authentication, integrity, and availability. Though these are critical requirements, they are insufficient in many applications. The communication patterns of sensors can, by themselves, reveal a great deal of contextual information, can disclose the location information of critical components in a sensor network. A sensor that detects this signal, the source sensor, then sends the location of pandas to a data sink (destination) with help of intermediate sensors. In general, any target-tracking sensor network is vulnerable to such attacks. As another example, in military applications, the enemy can observe the communications and locate all data sinks (e.g., base stations) in the field. Location privacy is, thus very important, especially in hostile environments. Failure to protect such information can completely subvert the intended purposes of sensor network applications. Location privacy measures, thus, need to be developed to prevent the adversary from determining the physical locations of source sensors and sinks. Due to the limited energy lifetime of battery-powered sensor nodes, these methods have to be energy efficient. Since communication in sensor networks is much more expensive than computation, we use communication cost to measure the energy consumption of our protocols.

An adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets and exploit the information like packet transmission time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. On the other hand, sensors usually have limited processing speed and energy supplies. It is very expensive to apply traditional anonymous communication techniques for hiding the communication between sensor nodes and sinks. So find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes as well as provide privacy preserving protocols for source and sink location in such sensor networks. The software used to simulate the proposed system is NS-2

II. WIRELESS SENSOR NETWORKS

A wireless sensor network is a collection of nodes organized in a network. Each node consists of one or more microcontrollers, CPUs or DSP chips, a memory and a RF transceiver, a power source such as batteries and

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

accommodates various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion.

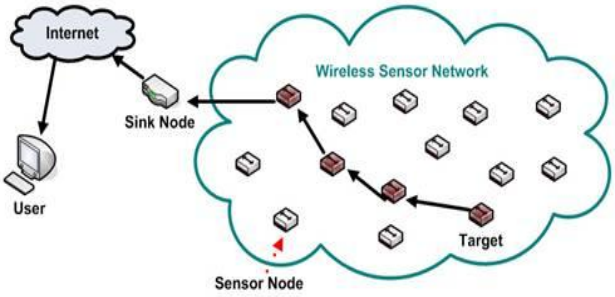

Figure1.Overview of Sensor Networks

A. Architecture of WSN

A Wireless Sensor Network (WSN) provides a low-cost and multifunctional means to link communications and computer networks to the physical world. It consists of base stations and a number of wireless sensors. Each sensor is a unit with wireless networking capability that can collect and process data independently. Sensors are used to monitor activities of objects in a specific field and transmit the information to the base station.

Sensor node

This is a mobile node moving freely to monitors the physical environment. Once it detects its physical target, it generates a data packet and sends it to the sink node via the wireless channel. The processor in the sensor node may be set the threshold value to compare with the detected data before it generates and sends a data packet.

Sink node

This node collects all data packets from sensor nodes and uses them to analyze their targets.

B. Node Structure

A sensor node can be divided into four basic modules: transducer, processor, communications and power. The transducer module contains the physical sensing device and an analog-to-digital converter (ADC). The sampled data is then passed to the processor, where it is stored in memory. Some applications merely require streaming of raw data while other applications require periodic sampling of the data.

However sophisticated applications require preprocessing of the data to extract important information so that transmission bandwidth can be preserved by simply transmitting the essential information (e.g., alerting the operator of a critical event). Local processing capability is also important for applications in which the sensor supports bidirectional communication.

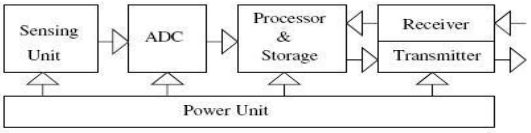

Figure2. Node Structure

In these cases, the users can query the sensor either for status or for a history of previous samples of data. The communication module consists of a short-range radio transceiver. The power module is used to house the battery and provides energy to the other modules. The functions of all four modules partially depend on the role of the sensor node. A sensor node can operate in one of the three roles: data collector, cluster head, or data relay.

If a node is a data collector, the transducer module directly passes the sampled data to the communication module for transmission. A cluster-head node gathers the sensed data from the cluster members and performs data processing to aggregate multiple signals into one signal. If a node works as a relay, it receives the data from nearby nodes and transmits the data to other nodes or the base station.

III. LOCATION PRIVACY ISSUES

1. Intercept network traffic due to the use of a broadcast medium for routing packets. Perform traffic analysis with packet transmission time and frequency.

2. Sensors have limited processing speed.

3. Sensor nodes have limited lifetime of battery.

4. Expensive traditional anonymous communication techniques for hiding the communication between sensor nodes and sinks.

5. Adversary (opponent) could deploy his own set of sensor nodes to monitor the communications in the target network.

6. Data are not encrypted after they reach a sink. So an adversary could locate sinks and make the sensor network nonfunctional by destroying them.

IV.EXISISTING APPROACHES

In this [9]Location Privacy in Sensor Networks Against a Global Eavesdropper, they analyze their effectiveness and evaluate their communication overhead in both analysis and simulation. They also show how these two schemes can be integrated together to meet the requirements of multi-application networks. Prior work on location privacy in sensor networks had assumed that the attacker has only a local eavesdropping capability. This assumption is unrealistic given a well-funded, highly-motivated attacker.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

- In this paper, they formalize the location privacy issues under the model of a global eavesdropper and show the minimum average communication overhead needed for achieving a given level of privacy.
- They also presented two techniques to provide privacy against a global eavesdropper. Analysis and simulation studies show that they can effectively and efficiently protect location privacy in sensor networks.

In location-based services, a user may want to retrieve location-based data without revealing the location. Techniques such as k-anonymity and private information retrieval have been developed for this purpose. However, there are some challenges unique to sensor networks. First, sensor nodes are usually battery powered, which limits their functional lifetime. Second, a sensor network is often significantly larger than the network in smart home or assisted living applications.

C. Source Location Privacy

Prior work in protecting location privacy to monitored objects sought to increase safety period, which is defined as the number of messages initiated by the current source sensor before a monitored object is traced. The coding technique requires a source node to send out each packet through numerous paths to a destination to make it difficult for an adversary to trace the source. However, the problem is that the destination will still receive packets from the shortest path first. The adversary can thus quickly trace the source node using backtracking. This method consumes a significant amount of energy without providing much privacy in return.

D. Destination Location Privacy

To protect the location privacy of destination from a local eavesdropper who is capable of carrying out time correlation and rate monitoring. First, they propose a multiple parents routing scheme in which for each packet a sensor no de selects one of its parents randomly and forwards the packet to that parent. This makes the trace pattern between the source and the destination more dispersed than the schemes where all the packets travel through same sequence of nodes. They also designed a scheme for creating some areas of high activity locally in the sensor network called hot spots. If such an area receives a packet, the packet has high probability of traveling through the same sequence of nodes creating an area of high activity. A local eavesdropper may be deceived into believing that this area is close to a destination.

V. PROPOSED SYSTEM

E. MAC Protocol Implementation

➢ A new MAC protocol, which is referred to as hybrid MAC (HMAC), which is suitable for WSNs in terms of energy efficiency, latency, and design complexity. HMAC combines channel-allocation schemes from existing contention-based and time-division multiple-access (TDMA)- based MAC protocols to allow the realization of tradeoffs between different performance metrics.

➢ It uses a short slotted frame structure and a novel wakeup scheme to achieve high-energy performance, low delivery latency, and improved channel utilization.

➢ Our proposed protocol (HMAC) combines energy-efficient features of the existing contention-based and time-division multiple access (TDMA)-based MAC protocols and adopts a short frame structure to expedite packet delivery

.

➢ HMAC is simple and scalable since each node does not have to maintain neighborhood information.

➢ HMAC provides routing layer coarse-grained quality- of-service (QoS) support at the MAC layer. To the best of our knowledge, very few existing MAC layer works handle such QoS issues in WSNs.

➢ Quality of service-aware medium access control assigns each flow a channel-access priority to reduce the queuing delay for high-priority flows but it still suffers from a long end-to-end delay.

➢ The MAC protocols presented in reduce the end-to-end delivery latency while increasing control overhead without considering different performance demands between flows

➢ Compromised source privacy can involuntarily leak source and sink location. The proposed system uses a scheme to hide source information using cryptographic techniques incurring lower overhead. The packet is modified by dynamically selected nodes to make it difficult for a malicious entity to trace back the packet to a source node and also prevent packet spoofing.

F.SPENA SCHEME

SPENA is a source-sink privacy protection scheme which uses one-way hash chains and mapping functions. SPENA uses a

1. One-way hash function to hide the source information and

2. Packet reconstruction strategy (rehashing scheme) to dynamically select the intermediate nodes on the packet path, which can protect source privacy under eavesdropping attacks while also tolerating node compromise attacks for altering the packet and

3. Packet verification method using the same one-way hash chain function is proposed for the base station to validate a received packet.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

The global eavesdropper compromises nodes to eavesdrop over the communication network which has access to all the cryptographic elements of the compromised node. The proposed system maintains source privacy under eavesdropping and node compromise attacks (SPENA). In this approach, encryption based method is used to increase source privacy. We use a one-way hash chain based keying mechanism to hide the source information. The one-way hash function generates a series of one-time use keys. This is further used to complicate an additional partial hash by dynamically selected nodes preventing a trace back by the adversary. The threat model considered allows the adversary to super-locally eavesdrop, while also being able to compromise nodes. When a node is compromised, the adversary has access to all the cryptographic information available to the node and also adversary has access to data packets of past communications stored at the compromised node.

1.Dynamic Source Routing

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. Dynamic Source Routing (DSR), is a reactive routing protocol that uses source routing to send packets. It uses source routing which means that the source must know the complete hop sequence to the destination. Each node maintains a route cache, where all routes it knows are stored. The route discovery process is initiated only if the desired route cannot be found in the route cache. To limit the number of route requests propagated, a node processes the route request message only if it has not already received the message and its address is not present in the route record of the message. DSR uses source routing, i.e. the source determines the complete sequence of hops that each packet should traverse. A negative consequence of this is the routing overhead every packet has to carry. However, one big advantage is that intermediate nodes can learn routes from the source routes in the packets they receive. Since finding a route is generally a costly operation in terms of time, bandwidth and energy, this is a strong argument for using source routing. Another advantage of source routing is that it avoids the need for up-to-date routing information in the intermediate nodes through which the packets are forwarded since all necessary routing information is included in the packets. Finally, it avoids routing loops easily because the complete route is determined by a single node instead of making the decision hop-by-hop.

2.Routing Protocal

The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on demand, allowing the routing packet overhead of DSR to scale automatically to only what is needed to react to changes in the routes currently in use. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example, for use in load balancing or for increased robustness.

DSR uses the key advantage of source routing. Intermediate nodes do not need to maintain up-to-date routing information in order to route the packets they forward. There is also no need for periodic routing advertisement messages, which will lead to reduce network bandwidth overhead, particularly during periods when little or no significant host movement is taking place.

VI.NETWORK DESIGNING

Performance Metrics : In order to evaluate the performance of wireless network routing protocols, the following parameters were considered:

1.Throughput

Throughput is the number of useful bits per unit of time forwarded by the network from a certain source address to a certain destination, excluding protocol overhead, and excluding retransmitted data packets. Throughput is the amount of digital data per time unit that is delivered over a physical or logical link, or that is passing through a certain network node.

Delivery Ratio = (Number of Packets Received) / (Number of packets Sent)

2.Delay

It is defined as the average time taken by the packet to reach the server node from the client node.
Delay = (Number of packets Received) / (Simulation Time)

3.Pause-time

It is the time for which a packet stops in when it reached a destination after a travel from the place of origination. The unit of pause-time is seconds.

4.Mobility

It is the velocity with which a node moves from the source to destination. It is usually specified in m/s.

5.Dropped packets

It is number of packets dropped due to the effect of link breaks. The dropped packets may be a control packets or data packets.

VII.SIMULATION AND RESULTS

NS-2 is a discrete event driven simulation software. The physical activities are translated to events. Events are queued and processed in the order of their scheduled occurrences Time progresses as the events are processed.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 4, April 2013

1.Simulation Parameters

The below parameters are configured in the network simulator. we use simulation to evaluate our techniques in terms of throughput and latency. we use a simulation model based on NS-2. The below parameters are configured in the network simulator.

TABLE1. SIMULATION PARAMETERS

Number of Nodes	30
Packet Size	250bytes
Terrain area	1800 * 1800
Mobility	10 m/s
Protocol used	DSR
Source node	6
Destination node	4

2.Packet Transmission

The protocol selects the shortest path from source node to destination node, without malicious node interference. Here the packets are transmitted from source node 6 to destination node 10 through the shortest path. Here the malicious nodes are 0,3,8,11,12,13,16.

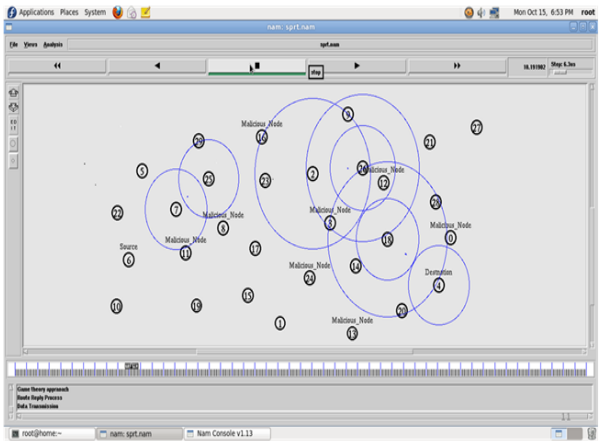

Figure 3. Simulation of Packet Transmission

3.Delay And Throuhput

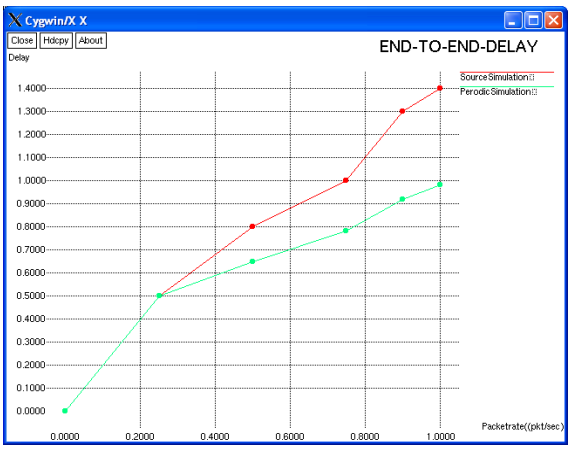

Fig.3.Delay vs packetrate(pkt/sec)

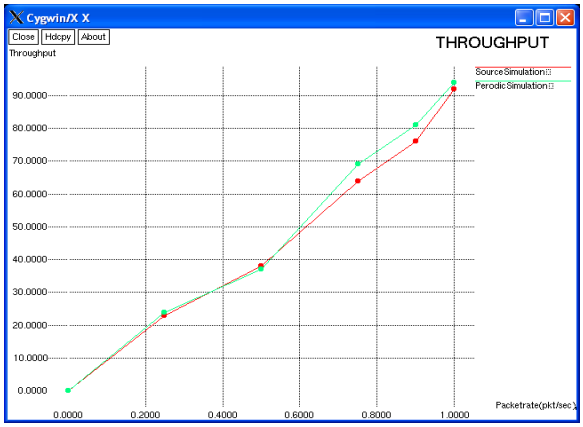

Fig.4.Throuput vs packetrate(pkt/sec)

VIII. CONCLUSION

In this paper, we formalized the location privacy issues under a global eavesdropper and estimated the minimum average communication overhead needed to achieve a given level of privacy. We also presented techniques to provide location privacy to objects and sinks against a global eavesdropper. We used analysis and simulation to show how well these techniques perform in dealing with a global eavesdropper. The results are analyzed and discussed in different terrain areas having networks of sensor nodes on varying Pause time for evaluating performance of different parameters like Packet Delivery Fraction, Average Throughput and Average End-to-end Delay in small, large and very large terrain areas. In the future, we will extend our study to networks with multiple sources and sink nodes.

REFERENCES

[1] Bamba.B, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacy grid," Proc. Int'l Conf. (WWW '08), 2008.

[2] Bollobas,B D. Gamarnik,O.Riordan, and B. Sudakov, "On the Value of a Random Minimum Weight Steiner Tree," Combinatorica, vol. 24, no. 2, pp. 187-207, 2004.

[3] Chan.H, A. Perrig, and D. Song, "Random Key Pre distribution Schemes for Sensor Networks,IEEE Symp. Security and Privacy (S&P '03), pp. 197-213, May 2003.

[4] Deng.J, R. Han, and S. Mishra, "Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '04),2004.

[5] Deng.J, R. Han, and S. Mishra, "Decorrelating Wireless Sensor Network Traffic Inhibit Traffic Analysis Attacks," Pervasive and Mobile Computing J., Special Issue on Security in Wireles MobileComputing Systems, vol. 2, pp. 159-186, Apr. 2006.

[6] Eschenauer.L and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks,"Proc. ACM Conf. Computer and Comm. Security (CCS '02), Nov. 2002.

[7] Ghinita.G P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.L. Tan, "Private Queries in Location Based Services: Anonymizers are not Necessary," Proc. ACM SIGMOD Int'l Conf. Management Data(SIGMOD '08), 2008.

[8] Kamat,.P Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," Proc. Int'l Conf. Distributed Computing System (ICDCS '05), June 2010

[9] Mehta.K, D. Liu, and M. Wright, "Location Privacy in Sensor Networks against a GlobalEavesdropper," Proc. IEEE Int'l Conf Network Protocols on mobile computing,February 2012.

[10]Mehta.K, D. Liu, and M. Wright, "Preventing Location on Sensor Networks against a Eavesdropper," IEEE Int'l Conf Network Protocols (ICNP '07), 2007.