IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, Sept 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

Collection of Data in Secure Way in Wireless Sensor Networks

Kiran Malik[1], Sunita[2]

[1]**Assistant Professor, M.R.I.E.M., Rohtak (India)**
kiransaggi2001@gmail.com

[2]**Assistant Professor, S.B.M.N. Engineering College, Rohtak (India)**
kashisuni5@gmail.com

Abstract

Wireless Sensor Networks make it possible to send secure data from source to destination. If applied to network monitoring data on a host, they can used to detect compromised node and denial-of-service is two key attacks. In this paper, we present four "Multi-path randomized routing Algorithm" a method to send the data multiple ways to classify the data in to normal and attacks in wireless sensor networks. The Pure Random Propagation shares are propagated based on one-hop neighborhood information, sink TTL initial value N in each share and remaining algorithms improve the efficiency of shares based on using two-hop neighborhood information. Our work studies the best algorithm by detecting the comprised nodes with black holes and denial of service in the packet information with Multipath routing algorithms that has not been used before. We analyses the algorithm that have the best efficiency and describes the proposed system.

Keywords: Wireless Sensor Networks, Security, Attacks and Routing.

I. Introduction

Wireless Sensor Networks typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communication capabilities [1], [2]. These sensor nodes communicate the distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control [3]. The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission.

In many WSN applications, the deployment of sensor nodes is performed in an ad hoc fashion without careful planning and engineering. Once deployed, the sensor nodes must be able to autonomously organize themselves into a wireless communication network. Sensor nodes are battery-powered and are expected to operate without attendance for a relatively long period of time. In most cases it is very difficult and even impossible to change or recharge batteries for the sensor nodes.

WSNs are characterized with denser levels of sensor node deployment, higher unreliability of sensor nodes, and sever power, computation, and memory constraints.

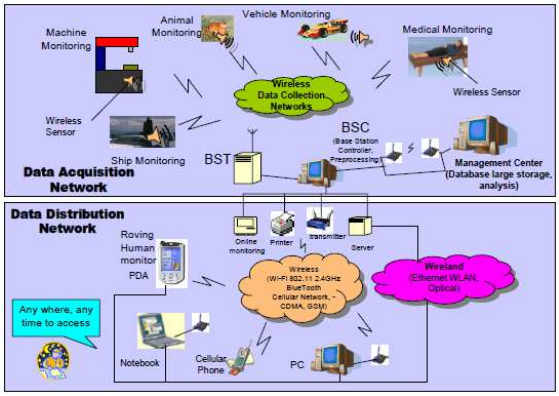

Fig.1. Examples of Wireless Sensor Networks

Thus, the unique characteristics and constraints present many new challenges for the development and application of WSNs.

Wireless sensor network (WSN) is a heterogeneous system combining millions of tiny, inexpensive sensor nodes with several distinguishing characteristics. It is low processing power and radio ranges, permitting very low energy consumption in the sensor nodes, and performing limited and specific sensing and monitoring functions [1], [2], [3], [4], [5], [6]. However, WSNs form a particular class of ad

hoc networks that operate with little infrastructure and have attracted researchers for its development and many potential civilian and military applications such as environmental monitoring, battlefield surveillance, and homeland security.

However, designing security protocols is a challenging task for a WSN because of the following unique characteristics:

Wireless channels are open to everyone and has a radio interface configured at the same frequency band. Thus, anyone can monitor or participate in the communication in a wireless channel. This provides a convenient way for attackers to break into a network.
A stronger security protocol costs more resources in sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off has to be made between security and performance. However, weak security protocols may be easily broken by attackers.

A WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment. Therefore, it may face various potential attacks.

II. Routing Protocols in WSN

Routing in wireless sensor networks differs from the conventional routing in fixed networks in various ways. There is no infrastructure, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet strict energy saving requirements [7]. All major routing protocols proposed for WSNs may be divided into seven categories.

A. Location-based Protocols

In location-based protocols, sensor nodes are addressed by means of their locations. Location information for sensor nodes is required for sensor networks by most of the routing protocols to calculate the distance between two particular nodes so that energy consumption can be estimated.

B. Data Centric Protocols

Data-centric protocols differ from traditional address-centric protocols in the manner that the data is sent from source sensors to the sink. In address-centric protocols, each source sensor that has the appropriate data responds by sending its data to the sink independently of all other sensors. However, in data-centric protocols, when the source sensors send their data to the sink, intermediate sensors can perform some form of aggregation on the data originating from multiple source sensors and send the aggregated data toward the sink. This process can result in energy savings because of less transmission required to send the data from the sources to the sink.

C. Hierarchical Protocols

Many research articles in the early years have explored hierarchical clustering in WSN from different perspectives [8]. Clustering is an energy-efficient communication protocol that can be used by the sensors to report their sensed data to the sink. In this section, we describe a sample of layered protocols in which a network is composed of several clumps (or clusters) of sensors. Each clump is managed by a special node, called cluster head, which is responsible for coordinating the data transmission activities of all sensors in its clump. As shown in Figure 2, a hierarchical approach breaks the network into clustered layers [55].

Nodes are grouped into clusters with a cluster head that has the responsibility of routing from the cluster to the other cluster heads or base stations. Data travel from a lower clustered layer to a higher one. Although, it hops from one node to another, but as it hops from one layer to another it covers larger distances. This moves the data faster to the base station. Clustering provides inherent optimization capabilities at the cluster heads.

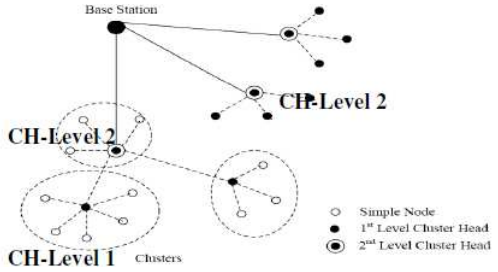

Figure 2 Cluster-based Hierarchical Model

D. Mobility-based Protocols

Mobility brings new challenges to routing protocols in WSNs. Sink mobility requires energy efficient protocols to guarantee data delivery originated from source sensors toward mobile sinks.

E. Multipath-based Protocols

Considering data transmission between source sensors and the sink, there are two routing paradigms: single-path routing and multipath routing. In single-path routing, each source sensor sends its data to the sink via the shortest path. In multipath routing, each source sensor finds the first k shortest paths to the sink and divides its load evenly among these paths.

F. Heterogeneity-based Protocols

In heterogeneity sensor network architecture, there are two types of sensors namely line-powered sensors which have no energy constraint, and the battery-powered sensors having limited lifetime, and hence should use their available energy efficiently by minimizing their potential of data communication and computation.

G. QOS-based Protocols

In addition to minimizing energy consumption, it is also important to consider quality of service (QOS) requirements in terms of delay, reliability, and fault tolerance in routing in WSNs.

III. Wireless Sensor Network Security Issues

Security mechanisms in WSN are developed in view of certain constraints. Among these, some are pre-defined security strategies, whereas some are direct consequences of the hardware limitations of sensor nodes.

A. Energy Efficiency

The requirement for energy efficiency suggests that in most cases computation is favored over communication and is three orders of magnitude more expensive than computation [9]. The requirement also suggests that security should never be overdone on the contrary; tolerance is generally preferred to over aggressive prevention [10]. More computationally intensive algorithms cannot be used to incorporate security due to energy considerations.

B. No Public-Key Cryptography

Public-key algorithms remain prohibitively expensive on sensor nodes both in terms of storage and energy [12]. No security schemes should rely on public-key cryptography. However it has been shown that authentication and key exchange protocols using optimized software implementations of public-key cryptography is very much viable for smaller networks [5].

C. Physically Tamper-able

Since sensor nodes are low-cost hardware that are not built with tamper-resistance in mind, their strength has to lie in their number. Even if a few nodes go down, the network survives. The network should instead be resilient to attacks. The concept of resilience, or equivalently, redundancy-based defense is widely demonstrated [10], [13], [11].

D. Multiple Layers of Defense

Security becomes an important concern because attacks can occur on different layers of a networking stack (as defined in the Open System Interconnect model). Naturally it is evident that a multiple layer of defense is required, i.e. a separate defense for each layer [10]. The issues mentioned here are in general.

IV. Security Requirements

A. Availability

Sensors are strongly constrained by many factors, e.g., limited computation and communication capabilities. Additional computations or communications consumes additional energy and if there is no more energy, data will not be available. Energy is another extremely limited resource in large scale wireless sensor networks. A single point failure will be introduced while using the central point scheme. This greatly threatens the availability of the network. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network [37]. Moreover, wireless sensor networks are vulnerable to various attacks. The adversary is

assumed to possess more resources such as powerful processors and expensive radio bandwidth than sensors. Equipped with richer resources, the adversary can launch even more serious attacks such as DOS attack, resource consumption attack and node compromise attack.

B. Confidentiality

Data confidentiality is the most important issue in network security. Confidentiality, integrity and authentication security services are required to thwart the attacks from adversaries mentioned in the above section. These security services are achieved by cryptographic primitives as the building blocks. Confidentiality means that unauthorized third parties cannot read information between two communicating parties. A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.

• In many applications, nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.

• Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. Generally, encryption is the most widely used mechanism to provide confidentiality.

C. Integrity and Authenticity

Confidentiality only ensures that data cannot be read by the third party, but it does not guarantee that data is unaltered or unchanged. Integrity means the message one receives is exactly what was sent and it was unaltered by unauthorized third parties or damaged during transmission. Wireless sensor networks use wireless broadcasting as communication method.

Thus it is more vulnerable to eavesdropping and message alteration [1]. Measures for protecting integrity are needed to detect message alteration and to reject injected message. Authentication ensures that the sender was entitled to create the message and that the contents of the message have not been altered. In the public key cryptography, digital signatures are used to seal a message as a means of authentication. In the symmetric key cryptography, MACs are used to provide authentication. When the receiver gets a message with a verified MAC, it is ensured that the message is from an original sender. Digital signature is based on asymmetric key cryptography (e.g., RSA), which involves much more computation overhead in signing/decrypting and verifying/encrypting operations. It is less resilient against DOS attacks since an attacker may feed a victim node with a large number of bogus signatures to exhaust the victim's computation resources for verifying them [10].

D. Data Freshness

Data freshness means that the data is recent and any old data has not been replayed. Data freshness criteria are a must in case of shared- key cryptography where the key needs to be refreshed over a period of time. An attacker may replay an old message to compromise the key.

E. Self Organization

Due to the ad-hoc nature of WSNs it should be flexible, resilient, adaptive and corrective in regards to security measures. The availability of small and cheap wireless sensing devices increased significantly in the past few years and large scale real-world sensor networks begin to appear. Such a large number of sensors deployed in the real-world allow for accurately monitoring a variety of physical phenomena, like weather conditions (temperature, humidity, atmospheric pressure etc) traffic levels on highways or rooms occupancy in public buildings. Making these sensors and their data available on a common web interface opens several interesting application scenarios. Users can query the available sensor B. Kumari et al. 53 data in real-time and use the query results to perform decisions or any kind of monitoring tasks. Since sensor data typically inherently relates to the specific sensor location, geo-based web interfaces like Google Maps or Windows Live Local are particularly suited to support real-world sensor querying.

Systems providing the necessary software infrastructure and tools for data acquisition, storage and online visualization of globally available sensor data begun to appear in the last few years. This master thesis will firstly survey and analyze these existing systems to outline which features they open to the users and to understand their usability. On the knowledge basis gained through this state-of-the-art survey, a simple framework for data acquisition, storage and visualization of sensor data will be

implemented, in order to provide an easy to- use prototyping environment for sensor-based applications. In particular, the framework will provide a tool for easily acquiring and storing data produced in wireless sensor networks and a web front-end based on Google maps to properly query and visualize the collected data. The prototype will be tested on an existing wireless sensor network deployment for urban noise monitoring.

V. Problem Definition

Nowadays, Compromised node and Denial-of-Service are two keys of attacks in wireless sensor networks (WSNs). Protection of sending the data from source to destination this model circumvents black holes formed by these attacks. For this, we explore the potential of random dispersion for information delivery in WSNs. Depending on the type of information available to a sensor; we develop our distributed scheme for propagating information "shares" called purely random propagation (PRP). PRP utilizes only one-hop neighborhood information and provides baseline performance. To diversify routes, an ideal random propagation algorithm would propagate shares as depressively as possible. PRP shares one-hop neighborhood information, a sensor node maintains a list of id's data of all nodes within its transmission range. When a source node wants to send shares to the sink, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and

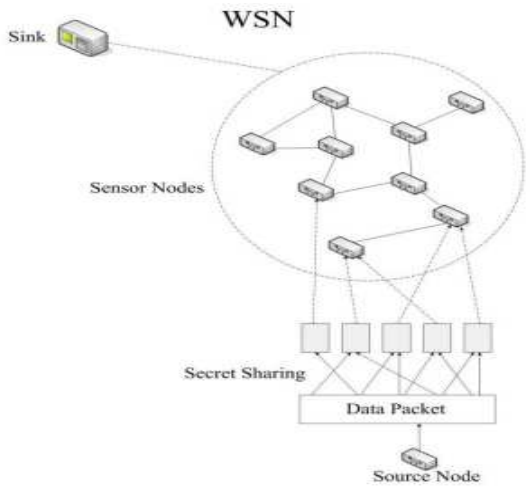

Figure 3 shows the collection data in wireless sensor networks

uni-casts the share to that neighbor. After receiving the share, the neighbor first decrements the TTL. If the new TTL is greater than 0, the neighbor randomly picks a node from its neighbor list (this node cannot be the source node) and relays the share to it, and so on.

Here the NRRP adds a "node-in-route" (NIR) field to the header of each share. Initially, this field is empty. Starting from the source node, whenever a node propagates the share to the next hop, the id of the upstream node is appended to the NIR field. Nodes included in NIR are excluded from the random pick at the next hop. Propagation efficiency improves by using two-hop neighborhood information, DRP adds a "last-hop neighbor list" (LHNL) field to the header of each share. Before a share is propagated to the next node, the relaying node first updates the LHNL field with its neighbor list. When the next node receives the share, it compares the LHNL field against its own neighbor list, and randomly picks one node from its neighbors that are not in the LHNL. It then decrements the TTL value, updates the LHNL field, and relays the share to the next hop, and so on.

VI. Usage of Random Multi-Path Routing Algorithms

A. Pure Random Propagation

Pure Random Propagation (PRP), shares are propagated based on one-hop neighborhood information. More specifically, a sensor node maintains a neighbor list, which contains the ids of all nodes within its transmission range.

When a source node wants to send data to destination, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and unicasts the share to that neighbor.

After receiving the share, the neighbor first decrements the TTL, if the new TTL is greater than 0, the neighbor randomly picks a node from its neighbor list (this node cannot be the source node) and relays the share to it, and so on. When the TTL reaches 0, the final node receiving this share stops the random propagation of this share, and starts routing it toward the sink using normal min-hop routing.

B. Non-Repetitive Random Propagation (NRRP)

Improves propagation efficiency by recording the nodes traversed so far:

– Adds node-in-route (NIR) field to the share header
– Initially NIR is empty at the source node
– When a share is propagated, the ID of the upstream node is added to the NIR field
– Nodes in NIR fields are excluded from random pick at the next hop
– Thus share is relayed to a different node in each step, leading to better propagation efficiency.

C. Directed Random Propagation (DRP)

Improves propagation efficiency with two hop neighborhood information:

– Adds last-hop-neighbor list (LHNL) field to the header of each share
– Propagating node updates the LHNL field before sending the share
– Receiving node compares this LHNL against its own LHNL & randomly picks a node that is not in LHNL of both nodes
– TTL value decremented, LHNL is updated, share relayed
– If the LHNL fully overlaps the relaying node LHNL, a random neighbor is selected, just like PRP.

• Benefits:

– Reduces the chance of propagating a share back and forth
– Better propagation efficiency as the share is pushed outwards

D. Multicast Tree Assisted Random Propagation (MTRP)

– Traditional location based routing algorithms

– Require location information at both the source and the destination and sometimes intermediate nodes (GPS at each node)

– Low accuracy of localization and high cost

– MTRP involves directionality in its propagation without needing location information

VII. Conclusion

In this paper a general Randomized multi-path routing algorithm for detecting comprised nodes and denial of service attacks in the packet information and an explanation mechanism to explain the computer network attacks results was described. The specific approaches of the black hole systems are characterized, we developed pure random propagation method is based on one-hope neighbor information shares. Our analysis has shown the effectiveness of the randomized dispersive routing in combating CN and DOS attacks. By appropriately setting the secret sharing and propagation parameters, the packet interception probability can be easily reduced by the proposed algorithms to as low as 10-3, which is at least one order of magnitude smaller than approaches that use deterministic node-disjoint multi-path routing. At the same time, we have also verified that this improved security performance comes at a reasonable cost of energy. Our current work does not address this attack. Its resolution requires us to extend, our mechanisms to handle multiple collaborating black holes, which will be studied in our future work.

References

[1] Shio Kumar Singh, M.P. Singh, and D.K. Singh, “A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks”, International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.
[2] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energyefficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Aug. 2010, vol. 2, no. 3, pp. 49-61.
[3] Shio Kumar Singh, M.P. Singh, and D.K. Singh, “Applications, Classifications, and Selections of Routing
[4] Protocols for Wireless Sensor Networks” International Journal of Advanced Engineering Sciences and Technologies (IJAEST), November 2010, vol. 1, issue no. 2, pp. 85-95.
[5] Shio Kumar Singh, M.P. Singh, and D.K. Singh, “Routing Protocols in Wireless Sensor Networks – A Survey” International Journal of Computer Science and Engineering Survey (IJCSES), November, 2011, Vol. 1, No. 2, pp. 63-83.
[6] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Performance Evaluation and Comparison of

Energy-efficient Routing Protocols for Wireless Sensor Network", Global Journal of Computer Application and Technology (GJCAT), Jan. 2011, vol. 1, no. 1, pp. 57-65.

[7] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy Efficient Transmission Error Recovery for Wireless Sensor Network", International Journal of Grid and Distributed Computing (IJGDC), December 2010, vol. 3, no. 4, pp. 89-104.

[8] S. Misra et al. (eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks, DOI: 10.1007/978- 1-84882-218-4 4, Springer-Verlag London Limited 2009.

[9] S.K. Singh, M.P. Singh, and D.K. Singh, "A survey of Energy- Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.

[10] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE International Conference on Pervasive.

[11] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[12] Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. Commun.ACM, 47(6):53{57, 2004. [12] D. Carman, B. Matt, D. Balenson, and P. Kruus, "A communications security architecture and cryptographic mechanisms for distributed sensor networks," in DARPA SensIT Workshop. NAI Labs, the Security Research Division Network Associates, Inc., 1999.

[13] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the 2003 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003.

[14] Shu, T.; Liu, S.; KrunzSecure, M. Data collection in wireless sensor networks using randomized dispersive routes. In Proceedings of IEEE INFOCOM Conference, Rio de Janeiro, Brazil, 19–25 August 2009, pp. 2846-2850.