Volume 6, Issue 6, June 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Role of Wireless Sensor Network in Data Security

Manju Yadav, Anu Rani
Yaduvanshi College of Engineering and Technology, Narnaul
Haryana, India

Abstract: ***In wireless sensor networks, sensor nodes can be compromised by intruders and the compromised nodes can distort data integrity by injecting false data. Data aggregation is essential to reduce data redundancy and to improve data accuracy, false data detection is critical to the provision of data integrity and efficient utilization of battery power and bandwidth. In addition to false data detection, data confidentiality is required by many sensor network applications to provide safeguards against eavesdropping.This proposed work integrates the detection of false data with data aggregation and confidentiality by using a verification algorithm. Data confidentiality prefers data to be encrypted at the source node and decrypted at the destination. However, in-network data aggregation techniques usually require an encrypted sensor data to be decrypted at data aggregators for aggregation. But in-network data aggregation could cause some security problems because a compromised data aggregator may inject false data during data aggregation. Tree-based aggregation approaches are not resilient to communication losses resulting from node and transmission failures, which are relatively common in WSNs. To address this problem, ring architecture is used which uses multipath routing techniques. A verification algorithm is used to compute aggregates and to enable the base station to verify if the computed aggregate is valid. It is an aggregate computation and verification algorithm.***

Keywords: Wireless, Sensor Network, Data Analysis, Algorithm, Data Integration.

I. INTRODUCTION

The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. Wireless networks are broadly divided into infrastructure and infrastructure less networks [1], where infrastructure network consists of wireless node with a network backbone and infrastructure less network consist with distributed, independent, dynamic topology, low-power, task –oriented wireless node. Cellular wireless network falls under the category of infrastructure network whereas ad-hoc and wireless sensor network (WSN) are the part of infrastructure less network [1]. In ad-hoc mode, the wireless devices integrated and communicated to each other by making an on-support dynamic wireless link.

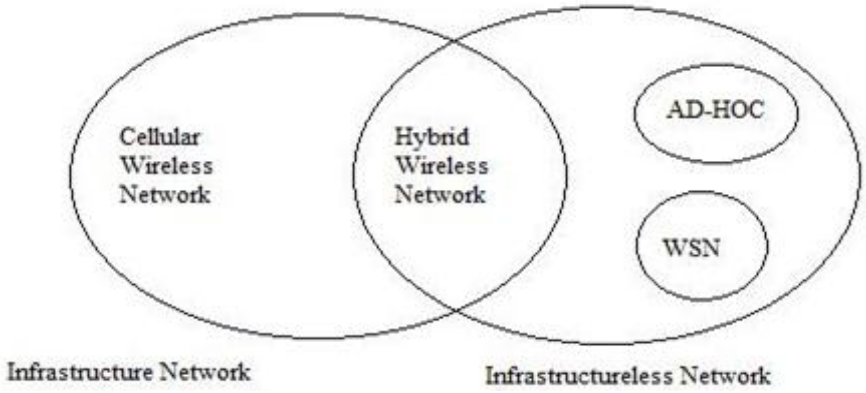

Figure 1.1 –Classification of Wireless Network

WSN consist with hundred/thousand wireless node distributed with geographical area;all wireless nodes collect information and supply towards central node for furtherprocessing. Recent advances in micro-electro- mechanical systems (MEMS) technology [2], wireless communications, and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes [2]. Sensor networks represent a significant improvement wireless sensor networks use small, low-cost embedded devices for a wide range of applications and do not rely on any pre-existing infrastructure. The vision is that these dives will cost less than $1. Sensors can be positioned far from the actual phenomenon [2] i.e. something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required. Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered [2].

1.1 Sensor Node Design

Sensing + CPU + Radio = Thousands of potential applications

Conceptually, a sensor node consists of a power unit, sensing unit, processing unit and radio unit that is able to both transmit and receive data. Sometimes the sensor node also has a mobility unit as well as a localization unit e.g. a global positioning system (GPS) [2].

1.1.1 Sensing

The sensing unit consists of two subunits, one or a group of sensors and an analog - to- digital converter (ADC) [3]. The ADC converts analog signals from the sensors to digital signals, used by the processing unit. The sensors are devices that respond to changes in the surroundings. The type of sensors being used on a sensor node depends on the application. The sensors can monitor speed, temperature, pressure, movement, humidity or vibrations etc.

1.1.2 Processing

The processing unit, usually a low speed CPU with small storage capabilities, performs tasks like routing and processing of sensed data etc. [4]. The choice of processing unit also determines, to a great deal, both the energy consumption as well as the computational capability of a sensor node.

1.1.3 Communication

The transmission between sensor nodes is wireless and can be implemented by radio, infrared or other optical media. Much of the current hardware for sensor nodes is based on radio link communication [5].

1.2 Sensor Networks Applications:

Sensor networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar, which are able to monitor a wide variety of ambient conditions that include the following[6]:

- Temperature
- Humidity
- Vehicular movement
- Lightning condition
- Pressure
- Soil makeup
- Noise levels
- The presence or absence of certain kinds of objects
- Mechanical stress levels on attached objects and
- The current characteristics such as speed, direction, and size of an object.

1.3 Network Design Objectives

Most sensor networks are application specific and have different application requirements. Thus, all or part of the following main design objective is considered in the design of sensor networks:

- **Small Node Size:** Since sensor nodes are usually deployed in a harsh orhostile environment in large numbers [2], reducing the node size can facilitate node deployment. It will also reduce the power consumption and cost of sensor nodes.
- **Low Node Cost*:*** Since sensor nodes are usually deployed in a harsh or hostileenvironment in large numbers and cannot be reused, reducing cost of sensor nodes is important and will result in the cost reduction of the whole network [2].
- **Low Power Consumption:** Since sensor nodes are powered by battery and itis often very difficult or even impossible to charge or recharge their batteries, it is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged [2].
- **Scalability:** Since the number sensor nodes in sensor networks are in the orderof tens, hundreds, or thousands, network protocols designed for sensor networks should be scalable to different network sizes [2].
- **Reliability:** Network protocols designed for sensor networks must provideerror control and correction mechanisms to ensure reliable data delivery over noisy, error-prone, and time-varying wireless channels [2].
- **Self-Configurability:** In sensor networks, once deployed, sensor nodes shouldbe able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures [2].
- **Adaptability:** In sensor networks, a node may fail, join, or move, whichwould result in changes in node density and network topology.
- **Channel Utilization:** Since sensor networks have limited bandwidthresources, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization [1].
- **Fault Tolerance:** Sensor nodes are prone to failures due to harsh deploymentenvironments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of self-testing, self-calibrating, self-repairing, and self-recovering [4].
- **Security:** A sensor network should introduce effective security mechanisms toprevent the data information in the network or a sensor node from unauthorized access or malicious attacks [2].

Other Commercial Applications:

Some of the commercial applications are monitoring material fatigue,building virtual keyboards, managing inventory, monitoring product quality, constructing smart office spaces, environmental control in office buildings, robot control and guidance in automatic manufacturing environments, interactive toys, interactive museums, factory process control and automation, monitoring disaster area, smart structures with sensor nodes embedded inside, machine diagnosis, transportation, factory instrumentation; local control of actuators, detecting and monitoring car thefts, vehicle tracking and detection, and instrumentation of semiconductor processing chambers, rotating machinery, wind tunnels, and anechoic chambers Environmental control in office buildings [7,8,9]. The air conditioning and heat of most buildings are centrally controlled.

II. ROUTING PROTOCOLS IN WSN

Routing in wireless sensor networks differs from conventional routing in fixed networks in various ways [2]. There is no infrastructure, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet strict energy saving requirements. Many routing algorithms were developed for wireless networks in general. All major routing protocols proposed for WSN may be divided into seven categories as shown in [2].

Category	Representative Protocols
Location-based Protocols	MECN, SMECN, GAF, GEAR, Span, TBF, BVGF, GeRaF
Data-centric Protocol	SPIN, Directed Diffusion, Rumor Routing, COUGAR,
	ACQUIRE, EAD, Information-Directed Routing,
	Gradient-Based Routing, Energy-aware Routing,
	Quorum-Based Information Dissemination, Home
	Agent Based Information Dissemination
Hierarchical Protocols	LEACH, PEGASIS,HEED,TEEN,APTEEN
Mobility-based Protocols	SEAD, TTDD, Joint Mobility and Routing, Data
	MULES,DynamicProxyTree-BaseData
	Dissemination
Multipath-based Protocols	Sensor-Disjoint Multipath, Braided Multipath, N-to-1
	Multipath Discovery
Heterogeneity-based Protocols	IDSQ, CADR, CHR
QoS-based Protocols	SAR, SPEED, Energy-aware routing

2.1 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. In this section, we present a sample of location-aware routing protocols proposed for WSNs [11].

2.2 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.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 [11]. This process can result in energy savings because of less transmission required to send the data from the sources to the sink. In this section, we review some of the data-centric routing protocols for WSN.

2.3 Hierarchical Protocols

Many research projects in the last few years have explored hierarchical clustering in WSN from a different perspective. Clustering is an energy-efficient communication protocol that can be used by the sensors to report their sensed data to the sink [5]. These protocols define that a network is composed of several clumps (or clusters) of sensors. Each clump is managed by a special node, called the cluster head, which is responsible for coordinating the data transmission activities of all sensors in its slump. A hierarchical approach breaks the network into clustered layers.

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 [11]. Data travels 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.

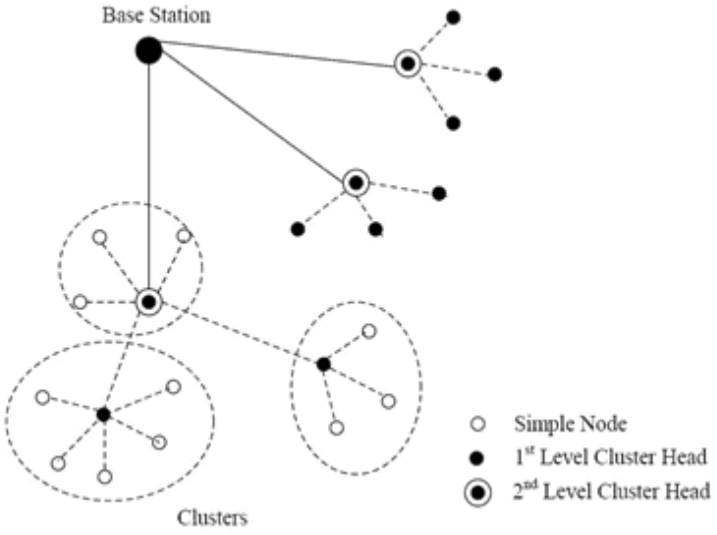

Figure 1.3: Hierarchical Protocol

2.4 Low-Energy Adaptive Clustering Hierarchy (LEACH):

LEACH [12] is the first and most popular energy-efficient hierarchical clustering algorithm for WSNs that was proposed for reducing power consumption. In LEACH [12], the clustering task is rotated among the nodes, based on duration. Direct communication is used by each cluster head (CH) to forward the data to the base station (BS). It uses clusters to prolong the life of the wireless sensor network. LEACH is based on an aggregation (or fusion) technique that combines or aggregates the original data into a smaller size of data that carry only meaningful information to all individual sensors. LEACH divides the a network into several clusters of sensors, which are constructed by using localized coordination and control not only to reduce the amount of data that are transmitted to the sink, but also to make routing and data dissemination more scalable and robust [12]. LEACH uses a randomize rotation of high-energy CH position rather than selecting in a static manner, to give a chance to all sensors to act as CHs and avoid the battery depletion of an individual sensor and dieing quickly.

2.5 Mobility-Based Protocols:

Mobility brings new challenges to routing protocols in WSN [10,14]. Sink mobility requires energy efficient protocols to guarantee data delivery originated from source sensors toward mobile sinks. In this section we discuss sample mobility-based routing protocols for mobile WSNs.

2.6 Multipath-Based Protocols:

Considering data transmission between source sensors and the sink, there are two routing paradigms [14]: 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. In this section, we review a sample of multipath routing protocols for WSNs.

2.7 Heterogeneity-Based Protocols:

In heterogeneity sensor network architecture [11,14] 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. The use of heterogeneity in WSN extends the network lifetime and present a few routing protocols.

2.8 QoS-Based Protocols:

In addition to minimizing energy consumption, it is also important to consider the quality of service (QoS) [2] requirements in terms of delay, reliability, and fault tolerance in routing in WSN. QoS based routing protocols helps in finding a balance between energy consumption and QoS requirements [14].

III. DATA AGGREGATION

In typical wireless sensor networks, sensor nodes are usually resource-constrained and battery-limited [2]. In order to save resources and energy, data must be aggregated to avoid overwhelming amounts of traffic in the network. There has been extensive work on data aggregation schemes in sensor networks. The aim of data aggregation is that eliminates redundant data transmission and enhances the lifetime of energy in wireless sensor network [2]. Data aggregation is the

process of one or several sensors then collects the detection result from other sensor. The collected data must be processed by sensor to reduce transmission burden before they are transmitted to the base station or sink.

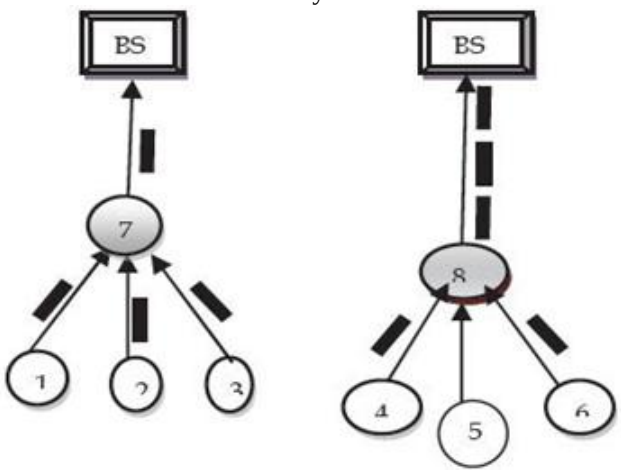

Figure 3.1: Data Aggregation

The wireless sensor network has consisted three types of nodes, Simple regular sensor nodes, aggregator node and querier [49]. Regular sensor nodes sense data packet from the environment and send to the aggregator nodes basically these aggregator nodes collect data from multiple sensor nodes of the network, aggregates the data packet using a some aggregation function like sum, average, count, max min and then sends aggregates result to upper aggregator node or the querier node who generate the query. It can be the base station or sometimes an external user who has permission to interact with the network. Data transmission between sensor nodes, aggregators and the querier consumes lot of energy in wireless sensor network. Figure 3.1 contain two models one is data aggregation model and second is non-data aggregation model in which sensor nodes 1,2,3,4,5,6,7,8 are regular nodes that collecting data packet and reporting them back to the upper nodes where sensor nodes 7,8 are aggregators that perform sensing and aggregating at the same time. In this aggregation model 4th data packet travelled within the network and only one data packet is transmitted to the base station (sink) and other non data aggregation model also 4th data packet travelled within the network and all data packets are sent to the base station (sink), means we can say that with the help of data aggregation process we decrease the number of data packet transmission and also save energy of the sensor node in the wireless sensor network [15]. With the help of data aggregation we enhance the lifetime of wireless sensor network. Sink have a data packet with energy efficient manner with minimum data latency.

3.1.1 Advantages and Disadvantages of Data aggregation in Wireless SensorNetwork

- **Advantages:** With the help of data aggregation process we can enhance therobustness and accuracy of information which is obtained by entire network, certain redundancy exists in the data collected from sensor nodes thus data fusion processing is needed to reduce the redundant information [13]. Another advantage is those reduces the traffic load and conserve energy of the sensors.
- **Disadvantages:** The cluster head means data aggregator nodes send fusethese data to the base station .this cluster head or aggregator node may be attacked by malicious attacker. If a cluster head is compromised, then the base station (sink) cannot be ensure the correctness of the aggregate data that has been send to it. Another drawback is existing systems are several copies of the aggregate result may be sent to the base station (sink) by uncompromised nodes .It increase the power consumed at these nodes [15].

IV. RESULTS

There are three rings and a base station or the sink node in the centre of the WSN network scenario. Sensor nodes are there to sense the change in the data. They generate the change in the usable data format by performing in network aggregation and will forward to the local synopsis or the computed data to the neighbouring nodes.

In the proposed three rings are used in which the ring which is nearer to the base station is ring of cluster heads and the next ring is an alternative path for the base station and the cluster head. If the cluster head dead then the transmission will be through the second ring and the third ring only senses the environment.

In the proposed technique, the main thing is that aggregation occurs in the form of circles or rings and the aggregation process automatically changes its route when an attack occurs in the network. Also, if any node dies in the ring then the network automatically connects itself to the most approachable node which is in the sensing range of the alive node. The main advantage of the proposed aggregation technique is that the aggregation process finds out its own way to reach the sink or base station.

V. CONCLUSION

A Wireless Sensor Network (WSN) is a set of sensors that are integrated with a physical environment. These sensors are small in size, and capable of sensing physical phenomena and processing them. They communicate in a multi hop manner, due to a short radio range, to form an ad hoc network capable of reporting network activities to a data collection

sink. Recent advances in WSNs have led to several new promising applications, including habitat monitoring, military target tracking, natural disaster relief, and health monitoring. The current version of sensor node, such as MICA2, uses a 16 bit, 8 MHz Texas Instruments MSP430 micro-controller with only 10 KB RAM, 128 KB program space, 512 KB external flash memory to store measurement data and is powered by two batteries. Due to these unique specifications and a lack of tamper-resistant hardware, devising security protocols for WSNs is complex. Previous studies show that data transmission consumes much more energy than computation.

VI. FUTURE SCOPE

- The proposed scheme is able to defend against the active attacks, however not included the passive attack. So it can be extended to the other security attacks.
- Battery consumption poses one of the challenging issues in the WSN network designing. During the data aggregation the node will require more power than the rest of the nodes. So aggregation selector and rotator mechanism can be developed that enable the load sharing.
- A new scheme can be proposed for less overhead, less computation and better security.

REFERENCES

[1] Ajay Jangra, Swati,Richa, Priyanka, "Wireless Sensor Network (WSN): Architectural Design issues and Challenges*",International Journal onComputer Science and Engineering (IJCSE), Vol. 02, No. 09,* 2010.

[2] I.F. Akyildiz, W.Su, Y.Sankarasubramaniam, E. Cayirci, "WirelessSensor Networks: A Survey*", IEEE commun. Mag., published by Elsevier ScienceB.V.,* 2002.

[3] C. Intanagonwiwat, R. Govindan, D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks", *Proceedings of theACM Mobi- Com'00, Boston, MA,* 2000, pp. 56–67.

[4] G.J. Pottie, W.J. Kaiser, "Wireless integrated network sensors" *Communications of the ACM 43 (5),* (2000) 551–558.

[5] E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, "A.Chandrakasan, Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks", *Proceedings of ACM MobiCom'01, Rome, Italy,* July2001, pp. 272–286.

[6] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, "Next century challenges: scalable coordination in sensor networks", *ACM MobiCom'99, Washingtion,USA,* 1999.

[7] N. Bulusu, D. Estrin, L. Girod, J. Heidemann, "Scalable coordination for wireless sensor networks: self-configuring localization systems", *InternationalSymposium on Communication Theory and Applications (ISCTA 2001), Ambleside, UK,* July 2001.

[8] J. Agre, L. Clare, "An integrated architecture for cooperative sensing networks", *IEEE Computer Magazine,* May 2000, 106–108.

[9] S. Cho, A. Chandrakasan, "Energy-efficient protocols for low duty cycle wireless microsensor", *Proceedings of the 33rd Annual Hawaii InternationalConference on System Sciences, Maui, HI Vol. 2* ,2000.

[10] B. Warneke, B. Liebowitz, K.S.J. Pister, "Smart dust: communicating with a cubic- millimeter computer', *IEEE Computer,* January 2001.

[11] S.R.BoselinPrabhu, S.Sophia, Professor, "A Survey of Adaptive Distributed Clustering Algorithms for Wireless Sensor Networks," *International Journalof Computer Science & Engineering Survey (IJCSES) Vol.2, No.4,* November,2011.

[12] J.M. Cramer, R.A. Scholtz, M.Z. Win, "On the analysis of UWB communication channels", *IEEE MILCOM'99,* 1999, pp. 1191–1195.

[13] KiranMaraiya, Kamal Kant, Nitin, "Wireless Sensor Network: A Review on Data Aggregation" ,*International Journal of Scientific & EngineeringResearch Volume 2, Issue 4, April -2011 1 ISSN 2229-5518 ,IJSER,* 2011.

[14] Shio Kumar Singh1, M P Singh, and D K Singh, "Routing Protocols in Wireless Sensor Networks–A Survey", *International Journal of ComputerScience & Engineering Survey (IJCSES) Vol.1, No.2,* November 2010.

[15] KiranMaraiya, Kamal Kant, Nitin Gupta, "Wireless Sensor Network: A Review on Data Aggregation", *International Journal of Scientific &Engineering Research Volume 2, Issue 4,* April -2011

