Survey on Wireless Sensor Networks

Article · January 2015

CITATIONS
0

READS
184

4 authors, including:

Hannan Ansari
KIIT University
4 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Survey on Wireless Sensor Networks

Hannan Ansari, Sachin Kumar Patel, Sachida Nanda Barik
School of Computer Engineering, KIIT University, Bhubaneswar, Orissa, India

***Abstract* - Wireless Sensor Networks are also a type of Network which has a small and large number of sensor nodes with limited sensing computation and communication capabilities. Basically WSNs are nothing but it is a type of network which has some sensing devices with communication capabilities. WSNs have some advantages and some disadvantages according to their use in different-different fields. To increase the life time of network, it is necessary to reduce the number of bits transmitted over the channel; if it happens then automatically the life time of network will increase. This paper introduces the Basic of WSNs, Security issues, and some techniques like data aggregation, for reducing the data transmission over the network is called data aggregation method. There are a lot of security issues in data aggregation for example data integrity, confidentiality and freshness in data aggregation. So data aggregation becomes a crucial when the WSN is deployed in remote environment or hostile environment where sensors are prone to node failure and compromises. Secure data aggregation schemes are fruitful to achieve the security in WSNs. In this paper, we propose a secure data aggregation schemes which provides end to end data privacy. Through this technique the average no. of bits transmitted per node is reduced by 35%-50%.**

***Keywords* - Computer Network, WSNs, Advance Computer Network, Intrusion Detection Systems, Network Security.**

I. INTRODUCTION

Wireless Sensor Networks has become popular network due to its unique attributes such as their light weight, low coast, small memory size, limited power and energies supply, and ad hoc nature. However WSNs is vulnerable to may attacks and the security can be affected by these attacks. WSNs have some problems like limited power, unreliable communication (e.g. unreliable transfer, conflict and latency) and unattended operation. So Researchers have started focusing on building a model that's name is "Sensor Trust Model" (STM) to solve these problems. And they have tried to resolve the challenges of maximizing the processing capabilities and energy reverse of wireless sensor nodes and also securing them against Viruses, Worms, hackers, and some malicious activities. Wireless Sensor networks and electronic enabled the development of low cost, low power, and multifunctional sensors nodes. These small sensor nodes consisting of sensing, data processing and communication components, and these attributes make it possible to deploy wireless sensor networks, which show some improvement over the traditional wireless sensor networks.

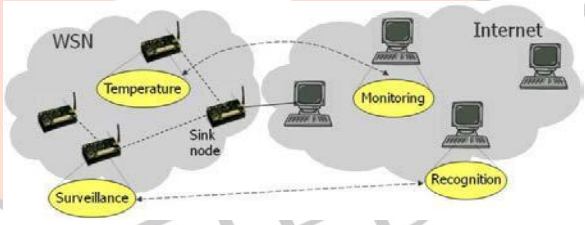

Figure-1, Relation between WSNs and Internet

WSNs are useful to many applications, such as:

a) It detects and tracts the passage of troops and tank on a battlefield.
b) It is monitoring the environmental pollutants.
c) It is measuring traffic flows on the roads.
d) It is tracking the location of personnel in a building.

Some aspects of Wireless Sensor Networks are similar to Traditional Wired ad-hoc Networks. There is some major difference between Sensor Network and ad hoc network are as given bellow [4]:

a) In Sensor networks, the number of the sensor nodes can be several ordered of magnitude and they are higher than the nodes in ad-hoc network.
b) Sensor nodes are densely deployed.
c) Sensors nodes are prone to failures due to harsh environments and energy constraints.
d) The topology of a sensor network changes very frequently due to failures or mobility.
e) Sensors nodes are limited in computation, memory, and power resources.

Merits of Wsns

There are lots of merits, which has been given bellow:

1. It has limited sensing computation and communication capabilities.
2. For better security purpose we can use a different type of Network that's name is Distributed Sensor Networks (DSNs).
3. Data freshness tells us that the data is new or recent, and also it ensures that no old messages have been replayed.
4. It also supports CIA concepts.
5. It becomes popular due to light weight, low coast, small memory size, limited power and energies supply, and ad hoc n ture.

Demerits of Wsns

WSNs have some demerits, which has been given bellow:

1. One of the biggest disadvantages of large scale wireless sensor networks lies on the complexity of logistics involving selective replacement of sensors that have ran out of energy.
2. Lower speed compared to wired network.
3. Less secure because hacker's laptop can act as Access Point. If you connected to their laptop, they'll read all your information (username, password, etc).
4. More complex to configure than wired network.
5. Affected by surrounding. e.g., walls (blocking), microwave oven (interference), far distance (attenuation) .
6. Gets distracted by various elements like Blue-tooth.
7. Still Costly at large.
8. It does not make sensing quantities in buildings easier.
9. It does not reduce costs for installation of sensors.
10. It does not allow us to do more than can be donwith a wired system.

II. NEED FOR SECURITY

In this field, we formalize the security properties require by Sensor Networks and it shows how they are directly applicable in a typical Sensor Network.

Data Confidentiality - The meaning of Data Confidentiality is that:" hide the essential or sensitive data from unauthorized users". Sensor Networks should not leak sensor readings to neighboring Networks. In this technique we encrypt sensitive data with the help of secret key that only intended receivers possess, hence achieving confidentiality.

Data Integrity - The meaning of data Integrity is that:"only authorized users can modify the sensitive data, unauthorized users or entity can't modify the sensitive data". The unauthorized user can modify the actual data then the sensor network send it into disarray i.e., a malicious node can add some fragments or manipulate the data within a packet. And this new packet can be sent to the original receiver. Information or data loss or damage can occur without presence of a malicious node due to harsh communication environment. So Data Integrity ensures that any received data has not been changed in transit.

Availability - The meaning of data Integrity is that:" only authorized users can access the sensitive data or information whenever they need to access". Unauthorized users can't access the sensitive data or information. Due to availability the data protection ensures. And Sensor Network should protect its resources from Intruders, Worms, Hackers, malicious activities and unauthorized users.

Data Freshness - According to key establishment process, each session key (shared key) fresh. The term data freshness tells us that the data is new or recent, and also it ensures that no old messages have been replayed. Key establishment has two forms of freshness guarantee, the first one is "weaker form" and second one is "stronger form".

Scalability - For better security purpose we can use a different type of Network that's name is Distributed Sensor Networks (DSNs). In distributed sensor networks, the numbers of nodes are 10 to 10,000. Small DSNs, can utilize a keying scheme but when we talk about large DNSs, large DSNs can't utilize keying scheme and it has a poor scaling properties either in the term of energy costs or latency. if we use multiple smaller subgroups with different group keys and when re-encrypt the actual message to forward from one subgroup to another. Hence this technique is so attractive when transmission energy costs are more important than computational costs.

Flexibility - Wireless Sensor Networks can be use in dynamic battlefield scenarios where some parameters may change rapidly like: environment conditions, threat, and mission. Two or more sensor networks can be combined into one and also a single sensor network can be split in two.

Self Organization - It is necessary in Wireless Sensor Network that every sensor node must be independent, flexible and self organize according to different situations. The infrastructure should be fixed in sensor network for the purpose of network management. But it is not available in sensor network. It is a lack point of WSNs. According to this inherent feature, there is a lot of great challenge to wireless sensor networks.

Threat Model - In WSNs**,** It is generally assumed that an attacker may know the all security vulnerabilities that are developed in a sensor networks. They may be able to communicate with a node or ever physically capture a node. When a node is suitable to access, then attacker starts stealing the key materials from that node. In the WSNs Base Stations are always treated as trustworthy, and many researchers are focusing only on secure routing between sensors and the Base Stations [4]. Some strategies against the threads are founded by Deng et al, the basic concepts of these strategies are: they lead the failure of the base station [10]. There are different-different types of attack in WSNs:

- Outsider Vs Insider attacks:
- Passive Vs Active attacks:
- Mote-class Vs Laptop-class attacks:

III. SECURITY VULNERABILITIES

The Sensor Networks are vulnerable for types of attacks, and such types of attacks can perform huge problems in WSNs through different-different ways. There are two types of securities vulnerabilities first one is passive attacks, and second one is active attacks.

1. Passive Attacks: A passive attack attempts to learn or make the use of information from hosts, it does not affect the system resources. The "Release of message contents" and "Traffic analysis" both comes in this type of attacks. [1]
2. Active Attacks: An active attack attempt to learn system resources and it also alter the system resources or effect their operation. The "masquerade", "Replay", "Modification of Messages", "Denial of Services" these types of attacks come in this section. [1]

Denial of Services attacks

This type of standards attacks on wireless sensor networks are jamming a node or set of node, the terms jamming of network has two forms: The first one is "Constant jamming" and the second one is "Intermittent jamming". In constant jamming, it involves the complete jamming of whole network; there are no facilities to send or receive messages. If the jamming is only intermittent, then the nodes can be able to exchange their messages periodically, but they can't consistently. Denial of Service is a type of active attacks. And active attacks involve some modification of data stream [5].

The Sybil attacks

This is the special type of attack in WSNs, why it is especial attacks in WSNs, because it is such type of case where a single node presents more than one identity to the network. It is able to defeat the redundancy mechanisms of "Distributed Data Storage systems" in peer to peer networks. In addition Sybil attacks are also effective against "Routing algorithms", "Data Aggregation", "Fair resources allocation", "foiling misbehavior detection" and "voting". Suppose a compromised node pretends to be two or three nodes, then the given algorithms used may conclude that redundancy has been achieved but in reality it has not. [4][5]

Traffic analysis attacks

Wireless Sensor Networks are basically a combination of low-power sensors communicating with some relatively robust and powerful base stations. It is not unusual, so all the gathered data by individual nodes are routed to the base stations. [5]

Privacy Violation:

In WSNs some more common attacks are fined against sensor privacy, and these are as:

- Monitor and Eavesdropping -Through meaning of the data, the hackers could easily discover the communication con-tents.
- Traffic analysis - It combines with monitoring and eavesdropping.
- Camouflage - The meaning of "Camouflage" is that, the adversaries can add their node in the sensor networks, and then thes nodes can masquerade as a normal node and attract the packets, and last it sends them in false direction.

IV. ARCHITECTURE OF WSNS FOR COMMUNICATION

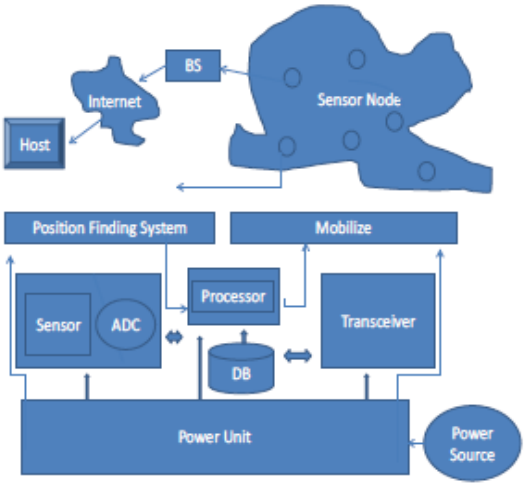

Figure 1. The Component of Sensor Node

WSNs are usually collection of hundreds or thousands of sensor nodes. These sensor nodes have capability to collect data and route data back to a Base Station (BS).A single sensor consists basically four parts: a sensing unit, a processing unit, a transceiver unit and last a power unit (Fig. 1). Sensing units are basically combination of two subunits: sensors and Analog to Digital Converters (ADCs). The work of ADCs is that it converts the analog signals into digital signals by the sensors. The work of processing unit is that, it manages the procedures that make the sensor node collaborate with the other nodes, and it generally associated with a small Storage Unit. The work of transceiver unit is that: it connects the node to the network. One of the most important units is power unit, power unit may be limited or infinite it totally depends on single batteries or may be supported by scavenging devices (e.g., solar cells). And mobilizer may sometimes need to move the sensor node, it totally depends on applications. There are a lot of protocol stack are used in sensor nodes, physical, data link, network, transport and application layers defined as follows: [4]

1. **Physical Layer**: This layer is responsible for signal deflection, modulation, and data encryption, selection of frequency and also for generation of carrier frequency.
2. **Data Link Layer** : This layer is responsible for multiplexing of data streams; data frame detection, medium access, and last error control, and also point to point, point to multipoint connections.
3. **Network Layer**: This layer is responsible for specifying the assignment of address, and the flow of packets.
4. **Transport Layer**: This layer is responsible for specifying how the reliable transport of packets will take place.
5. **Application Layer**: This layer is responsible for specifying how the data are requested and provided for both individual sensor nodes and interactions with the end user. [4]

V. ROUTING TECHNIQUES

In sensor Networks, there are two types of routing techniques are used the first one is flooding-based Routing and second one is single-path routing. And in this paper only flooding-bases routing is discussing

Flooding-based Routing: Many sensor networks employ flooding to disseminate data and control messages. In flooding, a message originator transmits its message to each of its neighbors, who in turn retransmit the message to each of their neighbors. Although flooding is known to have performance drawbacks, it nonetheless remains a popular technique for relaying information due to its ease of implementation, and the fact that minor modifications allow it to perform relatively well. In our baseline implementation of flooding, we have ensured that every node in the network only forwards a message once, and no node retransmits a message that it has previously transmitted. When a message reaches an intermediate node, the node first checks whether it has received that message before. If this is its first time, the node will broadcast the message to all its neighbors. Otherwise, it just discards the message. Realistically, this would require a cache at each sensor node. However, the cache size can be easily kept very small because we only need to store the sequence number of each message. We assume that each intermediate sensor node can successfully decrypt just the portion of the message corresponding to the sequence number to obtain the sequence number. Such an operation can easily be done using the CTR-mode of encryption. It is thus reasonable to expect that each sensor device will have enough cache to keep track of enough messages to determine whether it has seen a message before.[9][10][11].

VI. DISCUSSION

In this section we present a review of some of the recent security preserving Technique of WSNs.

In 2010 "Navin, A. Habibizad, Z. Navadad, B. Aasadi, and M. Mirnia", in their Research paper, "Encrypted Tag by Using Data-Oriented Random Number Generator to Increase Security in Wireless Sensor Network" In Computational Intelligence and Communication Networks (CICN), proposed to The main purpose of this paper is that to increase the security in wireless sensor networks by using Encrypted tag by using Data-Oriented Random Number Generator to encrypt tag of frames.

Data oriented is new technique and also applied theory which provides some methods that creates models the concepts with data structures. In this proposal there are two type of methods are used first one is interleaving Methods and second one is seed value in PRNG, and also the third one by initiating distributed of number banks. This paper has some disadvantages like: if we use data structure and cryptography techniques to develop some extra security for Wireless Sensor Networks then what about our new fresh data, where we will save these data or information, we must need a special memory to store the new fresh data which are provided by this concepts. [6]

In 2007 "Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti", in their Research paper, "A Survey on Wireless Sensor Networks Security." Proposed to the Sensor Network constraints, need of security, vulnerabilities of Security and also defensive methodologies of Wireless Sensors Networks. As we know that security requirements are critical in WSNs for data against adversary. So here this paper has been failed to provide 100% data security in WSNs.[5]

In 2006 "Wang, Yong, Garhan Attebury, and Byrav Ramamurthy" in their survey paper "A survey of security issues in wireless sensor networks", Proposed to the security issues in WSNs, types of attacks in WSNs, Defensive modes in WSNs, security provided by cryptography techniques; secure data aggregation, and finally, Intrusion detection techniques adopted by sensor networks.[4]

In 2014 "Marzi, Hosein, and Arash Marzi." in their Research paper "A security model for wireless sensor networks." In *Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*", Proposed to the enhanced mechanism of EBTRM, EBTRM is able to improve security label through increasing the accuracy. The optimum solution depends on Network infrastructure and management. When we compare two model "propose enhanced model" is able to find trustworthy sensors with large number of accuracy. And other hand "BTRM" operates less average distance between the client and selected sensors. [2]

In 2012 "Dr. Banta Singh Jangra, Vijeta Kumawat" in their Research paper "A Survey on Security Mechanisms and attacks in Wireless Sensor Networks", Proposed to the development of sensor nodes in an unattended environment, if Sensor nodes are developed in unattended environment, it will make the network vulnerabilities. This paper explains the attacks and their classification and also its security mechanisms. The three popular security solutions like; SPINS, TINYSEC AND LEAP which provides more security mechanisms to the WSNs. [3]

In 21 - 22 March, 2014 "Sukhchandan Randhawa "Research Challenges in Wireless Sensor Network: A State of the Play", proposed to the six key research areas including: localization, topology control, dependability, self-calibration, self-healing, data aggregation, group management, clock synchronization, query processing, sensor processing and fusion under limited capacities, and testing and debugging. [14]

VII. USEFUL TOOLS FOR WIRELESS SENSOR NETWORKS

In This section discussing about some latest WSN tools, there are several WSNs tools like: NS-2, TOSSIM, EmStar, OMNeT++, J-Sim, Avrora, Castalia. describes as follows:

NS-2 - The name of Network Simulator version-2, shortly called as NS-2. It has been developed in 1989 using for the purpose of Real Network Simulator (RNS). It is supported by "Defence Advance Research Agency" (DARPA) and National Science Foundation. One Special Characteristics of NS-2 is that, it is an open source simulator and it is a discrete event network simulator, which is based on Object-Oriented extension of tool command language and C++. It also can be run on Linux operating System and Cygwin. It is a popular non-specific network simulator can be used in both wire and wireless field. [15][16]

TOSSIM - It is an emulator, which is design for WSN and running on TinyOS platform, Which is an open source operating System. It was developed by UC Berkeley's TinyOS project team in 2003. It is a bit level discrete event emulator, which supports python and C++ language. We can run this emulator specially on linux OS or Cygwin on Windows. It also provides open source and online documentaion. [15][16]

Emstar - It is an emulator design for WSN usin c language. It is developed by University of California los Angles. It is a trace - driven emulator, which is runs on real time platform. It can also be run on Unix OS. This emulator supports to WSN Application based on better hardware sensors. [15][16]

OMNeT++ - OMNeT++ supports module programming model. It can run on Linux OS, Unix-like System and Windows. It is a popular non specific network simulator for both wire and wireless area. there are many simulation model and framworks in OMNeT++ used as Open Sources. [15][16]

J-Sim - J-Sim is a discrete event network simulator. It supports Java language. This Simulator provides GUI library. It is also provides open source models and online documents. This Simulator is widely used in the areas, like: physiology and biomedicine, but it also used in WSN simulation. [15][16]

Avrora - It is also a simualtor biult in java and design ffor WSN. It was developed by University of Calfornia, los Angles Com-

pilers Group. It provides a wide range of tools which can be used in wsn simulation. It has a additional propert, which combines the merits of TOSSIM and ATEMU. It does not provide GUI. [15][16]

CASTALIA - Castalia is a special type of simulator for WSN and similar network embedded systems, which is based on OMNeT++. It is a modulator and extended simulator, Using this simulator, Users are expected and assisted to create their own applications and protocols. It means the authenticated users can change the code of certain modules and also introduce new modules altogether.[15][16]

VIII. SUMMARY

A Wireless Sensor Network is a broad Network like traditional Computer Network. Here if we use multiple smaller subgroups with different group keys then we can use the 30% to 90% efficiency of the Network. When we send data from a one subgroup network to another one then we should re-encrypt the actual message and then forward. If we use such type of technique on Sensor Networks in WSNs we can improve the security chances. How we will secure data using some advance technologies in WSNs. Likes Data aggregation. Here we already mention the CIA properties; through these properties we can protect our sensitive data from unauthorized entity. The concept of this proposal is that how we secure the data in WSNs. Data aggregation schemes which provides end to end data privacy, So data aggregation schemes are fruitful to achieve the security in WSNs. A sensor network can secure and robust through its dynamic nodes, if we developed dynamic nodes that acts like a hosts as well as server then our network efficiency and workload of network can be manage. How it will happen in reality it is a great challenge for us. According to peer to peer networks concepts we can develop dynamic nodes which can perform both role like client as well as server. If particular node will perform both roles in simple manner then the data efficiency will automatically increase, then workload of channel will automatically decrease. We know that a particular node have some rights like; maintain the routing table, measures the flow of data, shortest path, and many more, but if we use some new technologies that will act on nodes then it will be good for sensor network, and what are the technologies we will enhanced in particular node. The name of technologies is Intrusion detection, Data aggregation. We will make IDSs for each and every node; these IDSs will do their job in simple manner. They will identify misused data or information whatever receive and send from one node to another node for conversation purpose.

REFERENCES

[1] Cryptography and Network Security: Principles and Practice, fifth Edition 2013 "*William Stallings*" published by Pearson Education, Inc, publishing as Prentice Hall, Copyright @ 2011.

[2] Marzi, Hosein, and Arash Marzi. "A security model for wireless sensor networks." In *Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2014 IEEE International Conference on*, pp. 64-69. IEEE, 2014.

[3] Jangra, Dr Banta Singh, and Vijeta Kumavat. "A Survey on Security Mechanisms and Attacks in Wireless Sensor Network." *International Journal of Engineering and Innovative Technology (IJEIT)* 2, no. 3 (2012): 291- 296.

[4] Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).

[5] Sharifnejad, Mona, Mohsen Sharifi, Mansoureh Ghiasabadi, and Sareh Beheshti. "A Survey on Wireless Sensor Networks Security." In *4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications (SEIT), TUNISIA, March 2007*. 2007.

[6] Navin, A. Habibizad, Z. Navadad, B. Aasadi, and M. Mirnia. "Encrypted Tag by Using Data-Oriented Random Number Generator to Increase Security in Wireless Sensor Network."

[7] In *Computational Intelligence and Communication Networks (CICN), 2010 International Conference on*, pp. 335-338. IEEE, 2010.

[8] Ren, Kui, et al. "On broadcast authentication in wireless sensor networks."Wireless Communications, IEEE Transactions on 6.11 (2007): 4136-4144.

[9] I. Akyildiz and I. Kasimoglu, "Wireless sensor and actor networks: Research challenges," *Ad Hoc Networks*, vol. 2, no. 8, pp. 351-367, 2004.

[10] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Department of Computer Science, University of Colorado, Tech. Report CU-CS-951-03, 2003.

[11] Al-Karaki, Jamal N., and Ahmed E. Kamal. "Routing techniques in wireless sensor networks: a survey." Wireless communications, IEEE 11.6 (2004): 6-28.

[12] Fasolo, Elena, et al. "In-network aggregation techniques for wireless sensor networks: a survey." Wireless Communications, IEEE 14.2 (2007): 70-87.

[13] Baronti, Paolo, et al. "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards." *Computer communications* 30.7 (2007): 1655-1695.

[14] Randhawa, Sukhchandan. "Research Challenges in Wireless Sensor Network: A State of the Play." *arXiv preprint arXiv:1404.1469* (2014).

[15] Siraj, S., A. Gupta, and R. Badgujar. "Network simulation tools survey." *International Journal of Advanced Research in Computer and Communication Engineering* 1.4 (2012): 199-206.

[16] Korkalainen, Marko, et al. "Survey of wireless sensor networks simulation tools for demanding applications." *Networking and Services, 2009. ICNS'09. Fifth International Conference on*. IEEE, 2009.