International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 9, September - 2013

Review on Evaluation & Challenges of wireless sensor network

Vinita Prashar
P.G Student in CSE Department,
Gurukul Vidyapeeth, Banur, Rajpura, Punjab, India

Aashima Bansal
Assistant Professor in CSE Department
Gurukul Vidyapeeth, Banur, Rajpura,Punjab, India

Satinder Pal Singh
Assistant Professor in CSE Department
Gurukul Vidyapeeth, Banur, Rajpura,Punjab, India

Abstract— Wireless Sensor Network is an Emerging Technology and very popular now a days due to its large and wide applications such as it is used in military, in disastrous areas, mountains, agriculture and many other areas for monitoring and tracking the information and the sensor nodes gather and provide information from available surrounding and perform local computation on them. Wireless Sensor Network is mainly madeup of 3 basic components i.e. a radio transceiver with internal and external antenna, microcontroller that provide interface with sensor nodes and a battery that provide energy to the whole network. But, there are many issues in wireless sensor network such as the energy consumption due to limited battery and also attacks on the wireless sensor network that make it inconvenient and insecure it due to these attacks. In this paper I am trying to introduce the main issues in wireless sensor network that provide the reason behind the energy waste and the attacks in the wireless sensor network this paper is just provide a introduction with some issues in wireless sensor network and also some existing system which try to overcome these problems .

Keywords— wireless sensor network, issues, attacks, energy conservation, existing system, applications

I. INTRODUCTION

The concept of wireless sensor networks is based on a simple equation as shown in fig1 Wireless sensor networks (WSNs) are ad-hoc networks that consist of hundreds to thousands of small sensor nodes communicating wirelessly to collect and deliver data to base stations. Once deployed, the small sensor nodes are usually Inaccessible to the user, and thus replacement of the energy source is not feasible. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.[1][13]

Fig-1 Concept of Wireless Sensor Network

II. Application Of wireless sensor networks:

Wireless sensor networks are most popular due to its wide range of application and these applications make it more popular and are able to monitor several information from available resources.

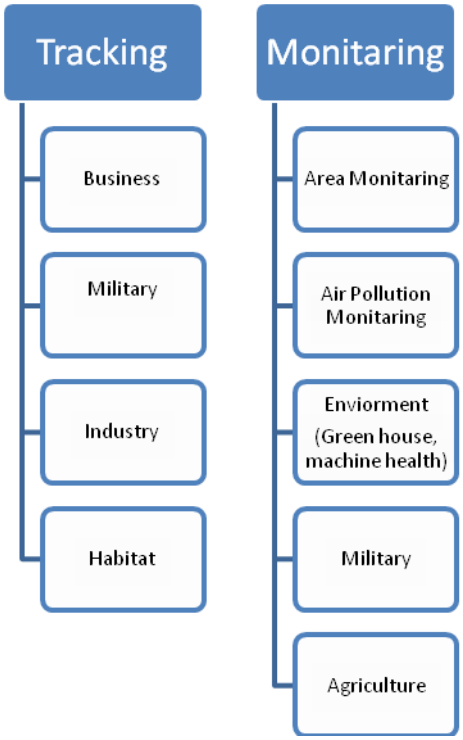


Fig-2 Applications of Wireless Sensor Network

APPLICATIONS USED

Area monitoring

In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors to detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.
Ex: a country at war with another may place nodes over a battlefield to detect enemy intrusion, sensors would detect heat, pressure, sound, light, electro-magnetic fields, vibrations, etc… If a sensor went off it would report it to a base station (message might be sent through internet or satellite).

Environmental Monitoring

In Environment monitoring, it is Similar to area monitoring where WSN is deployed over a region. Where some phenomena is to be monitored. Ex: coastal erosion, glacier monitoring

Air pollution monitoring

Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad-hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas.

Greenhouse monitoring

Wireless sensor networks are also used to control the temperature and humidity levels inside commercial greenhouses.

When the temperature and humidity drops below specific levels, the greenhouse manager must be notified.

Machine health monitoring

Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring.

Water/wastewater monitoring

There are many opportunities for using wireless sensor networks within the water/wastewater industries. Facilities not wired for power or data transmission can be monitored using industrial wireless I/O devices and sensors powered using solar panels or battery packs and also used in pollution control board.

Agriculture

Wireless network frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured.

III Basic Structure and Components of Wireless Sensor Networks:

Wireless sensor network is basically made up of nodes and with each node sensors are attached the combination are called as sensor node. These sensor nodes are communicate with each other and send whole data through a path called as gateway to the base station. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. Sensors are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure. Sensors measure physical data of the parameter to be monitored. The continual analogy signal produced by the sensors is digitized by an Analog-to-digital converter and sent to controllers for further processing. A sensor node should be small in size, consume extremely low energy, operate in high volumetric densities, be autonomous and operate unattended, and be adaptive to the environment. As wireless sensor nodes are typically very small electronic devices, they can only be equipped with a limited power source

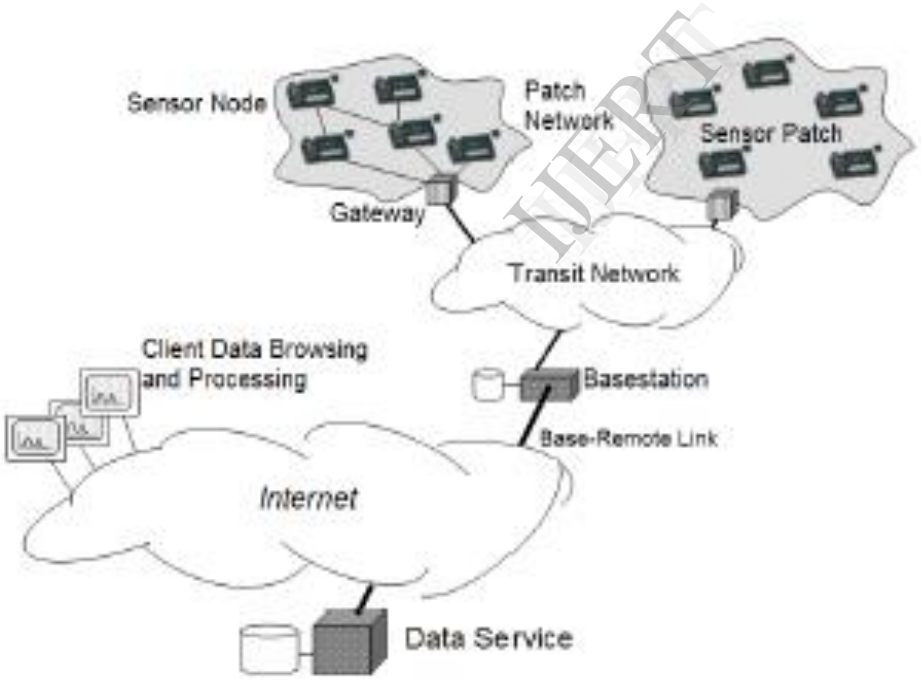


Fig – 3.1 Structure of Wireless Sensor Network

Figure shows the layout of a sensor networks where sensor nodes are used to collect the data which is passed through a transit network through multi –hops to reach the base station where the processing of data takes place and then it is forwarded to data service center for storage and analysis of the data collected takes place.

Sensor nodes: Any network consist of thousand of nodes and these nodes similarly wireless sensor network is also consist of thousand of nodes and with each node more than one sensors are attached theses are called as sensor nodes.
The basic components of sensor nodes are:
Sensing Unit: sensing unit are basically composed of 2 subunits sensors and analog to digital convertor the analog signal produced by sensors based on observed phenomena are converted to digital signal by ADC and then fed into the processing unit

Processing Unit: the processing unit is usually contain the small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks.

Transmission unit: A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit.

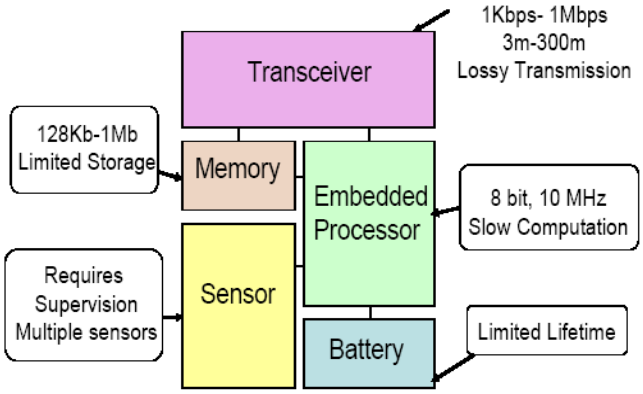


Fig-3.2 Component of Sensor Nodes

Power unit: Power units may be supported by a power scavenging unit such as solar cells. There are also other subunits, which are application dependent. Most of the sensor network routing techniques and sensing tasks require the knowledge of location with high accuracy. Thus, it is common that a sensor node has a location finding system. A mobilize may sometimes be needed to move sensor Nodes when it is required to carry out the assigned tasks. All of these subunits may need to fit into a matchbox-sized module.

IV Main Issues in Wireless Sensor Network:

a) Energy waste
b) Security attacks

A) Main Source of Energy Waste: Energy is a very scarce resource for such sensor systems and has to be managed wisely in order to extend the life of the sensor nodes for the duration of a particular mission. Energy consumption in a sensor node could be due to either "useful" or "wasteful" sources.

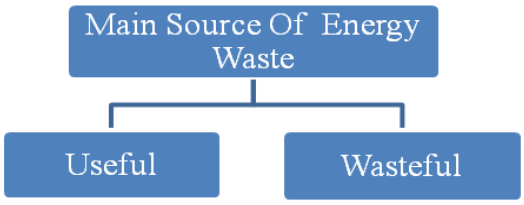


Fig-4 Type of Energy Waste

Useful Power Consumption:

1) Transmitting or resaving data.
2) Processing query request.
3) Forwarding Query or data to the neighbours.

Wasteful Power Consumption:

1) Idle listening of channel "wait for possible traffic".
2) Retransmitting because of Collisions "e.g. two packets arrived at same time at the same sensor".

3) "Overhearing" received a packet doesn't belong to it".
4) Generating And handling control packets.
5) "Over-emitting" when sensor received a packet while it is not ready.

Useful energy consumption can be due to transmitting or receiving data, processing query requests, and forwarding queries and data to neighbouring nodes. Wasteful energy consumption can be due to one or more of the following facts. One of the major sources of energy waste is idle listening, that is, (listening to an idle channel in order to receive possible traffic) and secondly reason for energy waste is collision (When a node receives more than one packet at the same time, these packets are termed collided), even when they coincide only partially. All packets that cause the collision have to be discarded and retransmissions of these packets are required which increase the energy consumption. The next reason for energy waste is overhearing (a node receives packets that are destined to other nodes). The fourth one occurs as a result of control-packet overhead (a minimal number of control packets should be used to make a data transmission). Finally, for energy waste is over emitting, which is caused by the transmission of a message when the destination node is not ready. Considering the above-mentioned facts, a correctly designed protocol must be considered to prevent these energy wastes.

V. Type of Attacks in network:

Type of attacks in network system is of two type and these attacks are:

a) Active attack
b) Passive attacks

Active attacks: - Attackers are try to break in to secure system this can be done trough viruses, worms and Trojan horses. In active attacks attacker are try to break protection features by introducing malicious codes or modify information e.g. Modification of data, men-in-middle attacks, Dos (Denial of service) attacks etc

Passive attacks: - A passive attacks monitors unencrypted traffic and looks for clear text passwords and sensitive information that can be used in other type of attacks this type of attacks include traffic analysis, monitoring of unprotected data or communication, decrypting weakly encrypting traffic and capturing authentication information such as passwords. Passive attacks disclosure of information and data files to an attackers without the knowledge of the user i.e. when attacker entity is unaware of the attacks, hence called passive attacks e.g. When attackers are just try to observe or listen you Similarly, in wireless sensor network the attacks are of many type witch challenge the security in wireless sensor networks

Type of Attacks and Security Threats in wireless sensor Networks:

1) **Dos Attacks**: Denial of service attack is a challenging attack in which someone tries to stop someone else from viewing part of internet. People who have Slower Internet connection such as dial –up connection are affected more by attacks. It is basically of 3 types Flood Attack**,** logic and software attack and distributed denial of service attack.[11][14]
2) **Sybil Attacks**: In Sybil Attacks create multiple identities (Sybil) and exploit them in orders to manipulate a reputation score. In this attacks attacker subverts the reputation of a peer to peer network by creating large number of identities. There are two ways to perform Sybil attacks. There are to ways to perform Sybil attacks one is to Sybil communicated directly with legitimate nodes .The other is that message send to Sybil node are routed through one of these malicious node that pretends to pass all the message to a Sybil node Sybil attacks can significantly reduce the effectiveness of multi path routing and pose a significant threat to geographical routing protocol.[12]

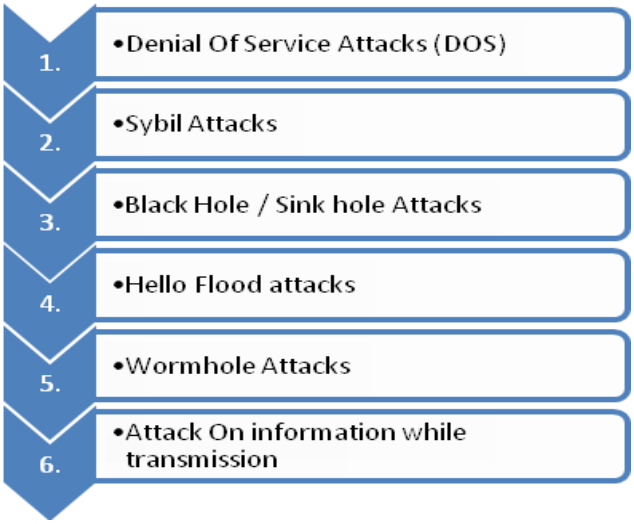


Fig-5 Type of Attacks in Wireless sensor network

Prevention: To prevent the Sybil attack, any node could check the list of "known-good" identities to validate another node as legitimate. The other solution is position Verification: the network verifies the physical position of each node. Sybil nodes can be detected using this approach because they will appear to be at exactly the same position as the malicious node that generates identities.

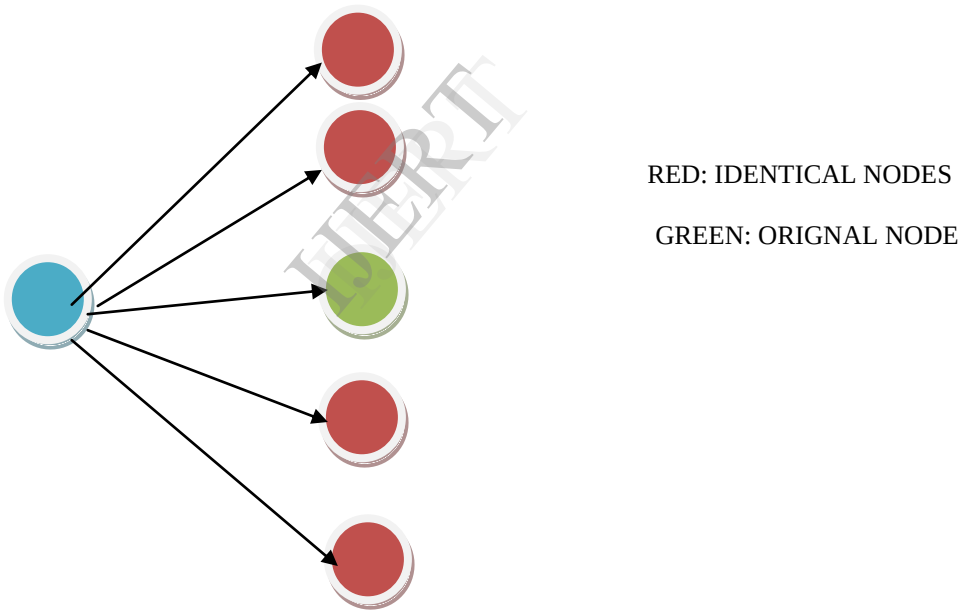
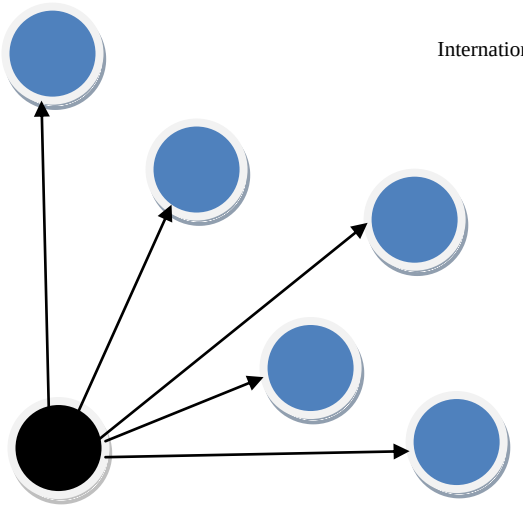


Fig: 5.1 The Sybil Attack

3) Black hole /Sink hole attacks: black hole refers to a place where incoming traffic is silently discarded without informing the source that the data did not reach the destination. In Wireless Sensor network all fake or malicious nodes act as a black hole and look especially very attractive to surrounding nodes it attack all the traffic especially in flooding based protocols attacker listen to the request of route that replies to the base station with the high quality and shortest path. Once the fake node enters between communicating nodes then i.e. between Sink and sensor nodes it can do anything with the packet passing between them and also affect the node that is away from base station the fig below shows representation of the black or sink hole in wireless sensor network [12]



Sink Hole

Fig- 5.2 Sink hole/ black hole attack

4) **Hello Flood Attack:** In Hello flood attack a malicious node can send, record or reply Hello message with high transmission power so That a large number of nodes even far away in the network choose it as a parent. It creates a illusion of being a neighbour to many nodes in the network and can confused the network routing badly. I n Hello Flood attacks it use a hello packet as a weapon to convince the sensor nodes in wireless sensor network. In this type of attack attacker have a high radio transmission (termed as laptop class attacker) it sends number of packets to the sensor nodes which are present in large area of wireless sensor network .In this attack each node update its routing information table and node update this table by sending and receiving hello and ACK message. When it attacker send the hello message to its neighbours then nodes update their tables and this attack increases delay [12]

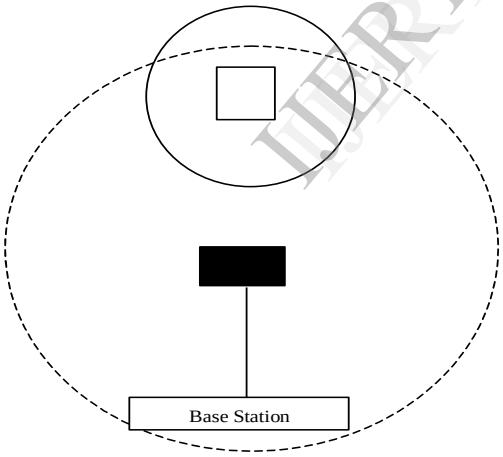


Fig-5.3 Hello Flood Attacks

5) **Wormhole Attacks:** Two powerful adversely nodes placed in two strategically location And advertise a low cost path to the sink. All nodes in the network are attract to them to find the optimal route. This attack is usually applied in conjunction with selective forwarding. The two adversely nodes advertise a route that two hops away. The adversaries are now in control of all the traffic in the network. The worm hole attacks are difficult to detect because communication medium between the two bad nodes are unknown. Control and verify hop count. This limits the self-organizing criteria of an ad-hoc network. Use protocol that is not based on hop count. In geographic routing, a route is based on coordinates of intermediate nodes. But if adversary nodes can mimic its location, this doesn't work.

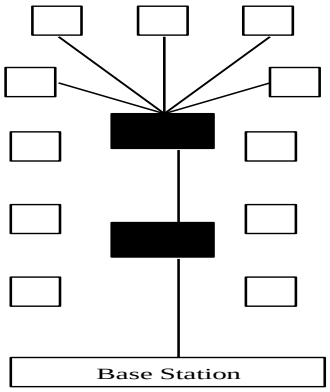


Fig-5.4 Hello Flood Attacks

Attack On information while transmission:
when sensor nodes are transiting its information to the sink or base station then the attackers interrupt on the transmission because the transmission range of the sensor nodes are typically low but the attackers are attack with the high transmission range and change or modify the original data with their own data and actual data does not reach at the sink . In this attack the attacker monitor the actual traffic and do changes in them during transmission.

VI Case Studies AND Related work

In this section we discuss various protocols proposed for security and energy of wireless sensor networks by different researchers.

1) SNEP Protocol

SNEP protocol [15] was designed as basic component of another protocol SPINS (Security protocol for wireless Sensor Networks) that was basically designed for secure key distribution in wireless sensor networks. SNEP define the primitives for authentication of sensor node, data confidentiality and data integrity.

Issues In Exciting System

However the drawback of this protocol is lower data freshness. SNEP protocol uses shared counter for semantic confidentiality not initial vectors. Using SNEP the plain text is ciphered with CTR encryption algorithm. Both sender and receivers are responsible to update the shared counter once when they sent or receive cipher blocks. Therefore sending counter in message is not important, however every message has message authentication code (MAC). This is computed from cipher data with the help of CBC-MAC algorithm. When the receiver node receives data it recomputed MAC and compared with the received MAC. If both are same it means data received in the packet is right.

2) TESLA with Instant Key Disclosure (TIK):

Y. C. Hu et al [16] proposed TIK protocol for controlling wormhole attack. This protocol is used for authentication of nodes in broadcast communication. TIK is extended form of TESLA protocol and it works on the basis of temporal lashes (efficient symmetric cryptographic primitives) that help the receivers to detect a wormhole attack. Message authentication code is computed with symmetric cryptographic primitives. TIK needs that there should be complete time synchronization between sender and receiver as well as use a single public key for scalable key distribution. There are three stages in TIL protocol.
i) Sender Setup: The sender uses a pseudo random function (PRF) to calculate master key and series of other keys. I also selects uniformly distributed points in time at which key is published like at T 0 disclose K 0 , T1 disclose K1 and so on. ii) Receiver Bootstrapping: All nodes have synchronized clocks and each receiver knows every sender hash root as well as other associated parameters which help him to authenticate a sender node. iii) Sending and verifying packets: For verifying packets the sender node calculates a key before sending packets on the basis of arrival time at destination. Using that key sender also send a MAC code with packet. The key is still secret although packet is received at destination. After receiving packet the key is transferred toward destination if the packet is verified correctly the packet must have originates from the claimed user.

Issues in existing system:
However a drawback of this protocol is authentication delay the receiver has to wait for sender key to authenticate a packet.

3) Pair wise key per-Distribution Scheme

W. Du et al [18] proposed a pair wise key distribution scheme for wireless sensor networks. The proposed scheme is totally based on Blom's key pre distribution scheme which allows any pair of nodes in the network to find a pair wise secret key. Pair wise keys enable nodes authentication,
increase network resilience and decrease communication and computation overhead. The author uses the concept of graph theory and draws an edge between two nodes if and only if they can find a secret key between themselves. There are few stages of pair wise key distribution scheme i. Key pre distribution phase in which key information is assigned to each node in the network. ii. Key agreement phase iii) Computing local connectivity and memory usage. This scheme is flexible and scalable as well as accepts the addition of new sensor nodes in later stages.

Issues in existing system:

However this scheme consumes more energy due to modular multiplication.

4) REWARD

Z. karakehayou [17] proposed a new algorithm know as REWARD for security against black hole attack as well as malicious nodes. It works on geographic routing. There are two different kinds of broadcast messages used by REWARD. MISS message helps in the identification of malicious sensor nodes. While the second message SAMBA is used to recognize the physical location of detected black hole attacks and broadcast that location. REWARD uses broadcast inter radio behaviour to observe neighbour node's transmission and detect black hole attack. Whenever any sensor misbehaves it maintain a distributed database and save its information for future use.

Issues in existing system:

However the main drawback of this protocol is high energy consumption.

5) Tiny Sec

Tiny Sec protocol [19] was proposed by C. Karlof et al for secure communication in resource limited wireless sensor networks. There are two types of security options in Tiny Sec.
i) Authenticated Encryption: In which the payload is encrypted and message authentication code (MAC) is used to authenticate a data packet. Where message authentication code is itself computed from packet header. For payload encryption 8 byte initial vector (IV) is used with cipher block chain (CBC). ii) Authentication Mode: The main difference in this mode and encrypted mode is that payload is not encrypted in simple authentication mode although authentication is done with the help of message authentication code.

6) Secure Data Aggregation

B. Przydatek et al [20] developed a framework for secure information aggregation in wireless sensor networks. The author used few sensor nodes as aggregator. These nodes aggregate information request which help to decrease communication overhead. The aggregator shares its results with home server and performs efficient interactive proofs. Where home server will be able to ensure results and detect any misconduct or any aggregator involve in cheating. Whenever the aggregator results are not similar to the home server results, the home server will recognize the attacker. In large sensor networks a single aggregator cannot handle the whole network therefore the set of aggregator nodes are used in hierarchical manner.

7) Statistical En-route Filtering

Ye et al. propose a statistical en-routing filtering mechanism called SEF. SEF requires that each sensing report be validated by multiple keyed message authenticated (MACs), each generated by a node that detects the same event. As the report being forwarded, each node along the way verifies the correctness of the MACs at earliest point. If the injected false data escapes the en-routing filtering and is delivered to the sink, the sink will further verify the correctness of each MAC carried in each report and reject false ones. To save the bandwidth, SEF adopts the bloom filter to reduce the MAC size. [9]

Issues in existing system

The filtering probability at each en-routing node is relatively low. Besides, SEF does not consider the possibility of en-routing nodes' compromise, which is also crucial to the false data filtering.

8) Hop-by-hop authentication (IHA)

Zhu et al. present an interleaved hop-by-hop authentication (IHA) scheme for filtering of injected false data. In IHA, each node is associated with two other nodes along the path, one is the lower association node, and the other is the upper association node. An en-routing node will forward receive report if it is successfully verified by its lower association node. To reduce the size of the report, the scheme compresses individual MACs.[10]

Issues in existing system

The security of the scheme is mainly contingent upon the creation of associations in the association discovery phase. Once the creation fails, the security cannot be guaranteed. The symmetric keys from a key pool, which allows the compromised nodes to abuse these keys to generate false reports.

9) Location-Based Resilient Secrecy (LBRS)

Yang et al. proposed Location-Based Resilient Secrecy (LBRS), which adopts location key binding mechanism to reduce the damage caused by node compromise, and further mitigate the false data generation in wireless sensor networks. [7]

Issues in existing system

To achieve en-routing filtering, additional 20 bytes authentication overheads are required.

10) Location-aware end-to-end data security design (LEDS)

Ren et al. propose more efficient location-aware end-to-end data security design (LEDS) to provide end-to-end security guarantee including efficient en-routing false data filtering capability and high-level assurance on data availability.

Issues in existing system

To achieve en-routing filtering, additional 20 bytes authentication overheads are required. It assumes that all the nodes can determine their locations and generate location-based keys in a short secure time slot.

11) Public key based solution

Zhang et al. provide a public key based solution to the same problem. Especially, they propose the notion of location-based keys by binding private keys of individual nodes to both their IDs and geographic locations and a suite of location-based compromise-tolerant security mechanisms.

12) Bit-compressed authentication technology

Bit-compressed authentication technology can achieve bandwidth-efficient. Canetti et al. use one-bit authentication to achieve multicast security. Source knows a set of keys each recipient u knows a subset. When the source sends a message M, it authenticates M with each of the keys, using a MAC.

Issues in existing system

In Bit-compressed authentication, however, once the source is compromised, the scheme obviously does not work. Therefore, it cannot be applied to filter false data injected by compromised nodes in wireless sensor networks.

13) BECAN SCHEME

A novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data is deployed in existing system. Based on the random graph characteristics of sensor node deployment and estimate the probability of k-neighbours which provides the necessary condition for cooperative bit-compressed BECAN authentication technique. This scheme saves energy by early detecting and filtering the majority of injected false data with minor extra overheads at the en-route nodes. In addition, only a very small fraction of injected false data needs to be checked by the sink which largely reduces the burden of the sink.

Issues in existing system

BECAN scheme is efficient for injecting false data by single attackers but not in case of group attackers. And has low reliability because if one report reaches the sink, the true event will successfully report else this scheme cannot filter injected false data. And if the path of length is too long authentication bit gets larger and hence reduce reliability as well as scalability.

VII Conclusion

In this paper we discussed security requirement for wireless sensor networks, we analyze different security threats and possible attacks as well as existing security approaches proposed by different researches with their basic characteristics. As WSNs grow in capability and are used more frequently, the need for security in them becomes more apparent. However, the nature of nodes in WSNs gives rise to constraints such as limited energy, processing capability, and storage capacity. These constraints make WSNs very different from traditional ad hoc wireless networks. While existing surveys or with related work discuss security and energy management in wireless Networks but still have some drawback in this article, we have surveyed the security issues in WSNs starting with the attacks While the discussed security services certainly add more computation, communication, and storage overhead in WSNs, and thus consume more energy, they are highly desirable and often required in real-world applications. However attack detection and prevention is still an important research area in wireless sensor network.

REFERENCES

[1] R. Szewczky, A. Mainwaring, J. Anderson, and D. Culler, "An Analysis of a Large Scale Habit Monitoring Application," Proc. Second ACM Int'l Conf. Embedded Networked Sensor Systems (Sensys '04), 2004.

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

[3] R. Lu, X. Lin, C. Zhang, H. Zhu, P. Ho, and X. Shen, "AICN: An Efficient Algorithm to Identify Compromised Nodes in Wireless Sensor Network," Proc. IEEE Int'l Conf. Comm. (ICC '08), May 2008.

[4] X. Lin, R. Lu, and X. Shen, "MDPA: Multidimensional Privacy- Preserving Aggregation Scheme for Wireless Sensor Networks," Wireless Comm. and Mobile Computing, vol. 10, pp. 843-856, 2010.

[5] X. Lin, "CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks," Proc. IEEE GLOBECOM '09, Nov.-Dec. 2009.

[6] K. Ren, W. Lou, and Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," Proc. IEEE Sensor Ad Hoc Comm. Networks (SECON '07), June 2007.

[7] L. Zhou and C. Ravishankar, "A Fault Localized Scheme for False Report Filtering in Sensor Networks," Proc. Int'l Conf. Pervasive Services, (ICPS '05), pp. 59-68, July 2005.

[8] Z. Zhu, Q. Tan, and P. Zhu, "An Effective Secure Routing for False Data Injection Attack in Wireless Sensor Network," Proc. 10th Asia-Pacific Network Operations and Management Symp. (APNOMS '07), pp. 457-465, 2007.

[9] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM '04, Mar. 2004.

[10] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by- Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[11] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong,"Security in Wireless Sensor Networks: Issues and Challenges**",**International conference on Advanced Computing Technologies**,** Page1043-1045, year 2006

[12] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003

[13] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002

[14] A.D. Wood and J.A. Stankovic (2002), ―Denial of service in sensor networks‖, IEEE Computer, Vol. 35, No. 10, pp. 54-62.

[15] L. Tobarra, D. Cazorla, F. Cuartero, Formal Analysis of Sensor Network Encryption Protocol (SNEP) IEEE International Conference on Mobile Ad-hoc and Sensor Systems, MASS 2007, PISA, 8-11 Oct. 2007.

[16] Y. C. Hu., A. Perrig, D. B. Johnson, Packet Leashes. A Defence against Wormhole Attacks in Wireless Networks 22nd Annual Conference of IEEE Computer and Communication Societies, IEEE 2003, pp, 1976-1986, 3 April, 2003.

[17] Z. Karakehayov, Using REWARD, to Detect Team Balckhole Attacks in Wireless sensor Networks Workshop on Real world Wireless Sensor Networks, (REAL WSN, 05) Stockholm, Swedan, June 2005.

[18] W. Du, J. Deng, S. Han, P. K. Varshney, A Pairwise Key Predistribution scheme for Wireless Sensor Networks Proceeding of ACM international Conference on Computer and Communication Security, pp, 42-51, 2003.

[19] C. Karlof, N. Sandy, D. Wagner, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks In Proceeding. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 2004.

[20] B. Przydatek, D. Song, A. Perrig, SIA: Secure information aggregation in Sensor Networks Proceedings of International conference on Embedded Networked Sensor Systems.-ACM,-pp.-255-265,-2003.