ORIGINAL RESEARCH PAPER

Engineering

Volume : 6 | Issue : 9 | September 2016 | ISSN - 2249-555X | IF : 3.919 | IC Value : 74.50

# Detection of Milicious Node Wireless Sensor Network

KEYWORDS

WSN;CH; BS; LEACH; SDAF; TESDA

**P.Padmaja**

Asst.professor,ECE Dept., VITS,Deshmukhi, Hyderabad, INDIA.

**Dr.G.V.Marutheswar**

Professor, Dept of EEE, S.V.U.College of Engineering, Tirupati, Andhra Pradesh,India

**ABSTRACT** *optimization Wireless Sensor Network (WSN) is necessary to reduce redundancy and energy consumption. To optimizing wireless sensor networks for secured data transmission both at cluster head and base station data aggregation is needed.Data aggregation is performed in every router while forwarding data. The life time of sensor network reduces because of employing energy inefficient nodes for data aggregation. Hence aggregation process in WSN should be optimized in energy efficient manner. So introduced one protocol on trust based with weights.This paper completely about theattacks,and some methods for secured data transmission.*

## Introduction

A sensor the asymmetric communication between a base station located anywhere in the network and the sensor nodes extend the life span of large centralized wireless sensor networks, It is also illustrated that enforcing a minimum separation distance between cluster heads amongst the clusters in a cluster based wireless sensor network, prolongs network lifespan. Besides, this work exhibits that for various types of applications related to wireless sensor network, the preference of heuristic algorithm is more important to prolong wireless sensor network lifespan than for other types of applications. Wireless sensor networks are swiftly becoming common in application areas where information from many sensor nodes is to be collected and acted upon. The deployment or implementation of wireless sensor networks adds flexibility to the network, and the additional cost of installation of cables can be avoided. Wireless sensor networks consist of many small compact devices, equipped with sensor nodes for many applications like acoustic, seismic or image sensors that form a wireless network. Each sensor node in the network collects information from its surroundings, and sends the sensed data to a base station, either from sensor node to sensor node under multi-hop,or directly to a base station under single-hop data communication. the acceptable power consumption, [2] of a variety of computing platforms. It can be seen that nodes are expected to consume at most 50mW, with considerably less being a particularly attractive proposition. Energy consumption is of prime importance in WSNs, and algorithms and hardware should be designed with energy-efficiency or energy-awareness as a central constraint, Vidhyapriya & Vanathi (2007).

## Issues of Data Aggregation

A network of energy-constrained sensors deploying over a region is considered, in that each sensor monitors its surrounding area and periodically generates nformation. The systematic gathering and transmission of sensed data to a base station for further processing is the basic operation in such a network.Sensors have the ability to carry out in-network aggregation or fusion of data packets reroute to the base station when data gathering. In such sensor system, the lifetime is the time in which the information can be gathered from all the sensors to the base station.In data gathering, from agreed energy constraints of the sensors expanding the system lifetime is a major threat [14]. The data aggregator node or the cluster head combine the data to the base station and the malicious attacker may attack this cluster node. The base station cannot ensure the accuracy of the aggregate data sent to it, if a cluster head is compromised. Due to the uncompromised nodes, the existing systems may send several copies of aggregate results to the base station and the power consumption at these nodes is increased [10].Compared to external attacks, internal attacks are hard to detect and prevent, thus raising more security challenges. Compromised nodes can launch the attacks are of Stealing secrets from the encrypted data which passed through it. Report wrong or false information to the network.Report other normal nodes as compromised nodes.Breach routing by introducing many routing attacks such as selective forwarding, black hole, modifying the routing data etc., while systems find it hard to notice these activities, and normal encryption methods have no effect to prevent them,because they own the secret information such as keys. Exhibit arbitrary behavior and may collude with other compromised nodes.

## SECURITY GOALS FOR WIRELESS SENSOR NETWORKS

In Application Layer the type of attack is Subversion and Malicious Nodes. Counter Measure of that is Malicious Node Detection and Isolation.In Network Layer the type of attack is Wormholes, Sinkholes, Sybil.counter .Measure of that is Key Management, Secure Routing ,In Data Link Layer the attack type is Layer Encryption.In Physical Layer the type of attack is DoS and Node.counter measure is capture.counter measure is Adaptive antennas, Spread Spectrum.

## Physical Attacks

Physical Attacks In a physical attack, the attacker gains direct access to the computing device hardware. This makes a denial-of-service attack easily possible: the attacker can simply destroy the sensor nodes. Physical access also allows him to access a node's components without any software layer involved. This is in contrast to a remote attack, where the attacked computer is accessed through some protocol or application layer, which gives it the possibility (at least, in principle) to detect the attack and react accordingly. In a physical attack, this sort of "self-surveillance" is not available to the device under attack and would only be possible by additional measures, such as external surveillance. This makes physical attacks extremely powerful.

They have a number of potential advantages over remote attacks:

• The attacker has (almost) certain knowledge about which device he is actually attacking. Network traffic, which is the medium for remote attacks, can be misdirected easily, and verifying the identity of a remote entity is hard. Physical attacks happen with direct access to the computer equipment, which usually gives enough information for reliably identifying the equipment itself and its owner. Once the attacker has gotten so close, it might be impossible to divert his efforts to a less sensitive target.

• Network traffic is often secured by cryptographic means, for example by employing SSL. This makes eavesdropping or message injection practically impossible. On computers, data can be stored in encrypted form as well, but this is often refrained from due to usability and availability issues (e.g. the danger of lost keys). Therefore, physical access to a computer system usually yields full access to the stored data herein, including the ability for manipulations.

• The closer one gets to a computer system, the higher becomes the available bandwidth. Remote attacks are constrained by network interfaces. A long-distance connection typically yields between 64 kbit/s and 2Mbit/s (ISDN, ADSL). Wireless connections usually yield between 128 kbit/s (ZigBee) and 54 Mbit/s (IEEE 802.11g). An attack occurring within a LAN yields up to 1 Gbit/s. Direct wired interfaces allow similar data rates, for example Firewire (the IEEE 1394b standard yields up to 800Mbit/s) or serial ATA (300 Mbyte/s = 2.4 Gbit/s).

• Sensitive information, which would not be accessible otherwise, can be acquired through special equipment that is secretly attached to a computer, e.g. a key logger for recording passwords.

• Physical evidence can be collected during an attack, which is not possible with remote attacks. Physical evidence could support non-repudiable attribution of data to a person or organization, thereby facilitating extortion. Examples of such evidence include hard disks, possibly with fingerprints on them, or printouts (that can be attributed to a certain printer).

On the other hand, physical attacks are usually riskier than remote attacks, since the attacker himself enters the domain of his opponent. Some risks are:

• Leaving traces that could lead to the identification of the attacker.

• Physical effort is required to break into the area where the computers are kept (e.g. a server room), which is susceptible to detection my surveillance mechanisms. Physically attacking a sensor network avoids most of the risks usually associated with physical attacks. Sensor nodes are usually placed outside the close domain of their owners, for example in public spaces. Surveillance systems may be hard to operate in such areas. Once the attacker has physical access to the sensor nodes, it is easy for him to extract information from them if no further precautions are taken. One possible measure is tamper-proofing. Here, sensor nodes are shielded by a barrier that is hard to penetrate and thereby prevents direct access to memory or the CPU. Similarly to smart cards or trusted platform modules (TPM), the core computational unit concerned with the handling of secret keys could be made tamper-resistant. This may deter an occasional attacker, but a determined and resourceful attacker is likely to break any existing shielding or scrambling mechanism as research in smart cards and other hardware platforms (such as the X-Box gaming console. Active countermeasures can further raise the bar for the attacker, for example by incorporating means for detecting a physical breach, temperature extremes, voltage variation, and radiation, which is common in high-end security modules.As soon as a potentially threatening event is detected, the memory holding secret keys is zeroed. Such measures are costly, and an acceptable trade-off must be found that takes the actual risk of such attacks into account. Sensor devices, which have to be available in large quantities at low cost, are unlikely to incorporate such means. However, a certain level of self-protection may be possible. The sensors that are already attached to a sensor device may be useful for detecting certain events, for example sudden movements, which may be sufficient for many practical applications. If tamper resistance is considered too costly, at least some level of tamper evidence may be provided. Upon inspection, this would make the fact that an attack has occurred obvious. Natural characteristics of the deployment area may also support the protection of a sensor network. For example, the terrain where the nodes are placed may be inaccessible, or sensor nodes may be concealed between other objects, making them harder to detect. All these measures lead to a certain level of tamper resilience, which increases the cost for a successful attack, for example by delaying the attacker or requiring him to acquire specially crafted equipment. The risk of a physical attack depends on the environment and the context in which the sensor network is deployed. Questions to consider in order to assess the risks are: Who would be interested in disabling the network? Where and when is the network deployed, and how high is the exposure to potential attackers? What is the potential impact of a disabled or manipulated sensor network? In many cases, one might be satisfied with the risk being reduced by inherent properties of sensor networks, i.e. the small size and high redundancy of sensor devices

**Interface attacks**

Interface attacks exploit vulnerabilities of the interfaces a device provides in order to allow access to its own services or to access external services. For wireless communication interfaces, there are obvious attacks such as eavesdropping, jamming, traffic analysis, and message injection among others. They are facilitated by the broadcast nature of wireless communication, and the fact that access is easily possible without the risk of detection. An overview can be found, e.g., in . Interface attacks can also be executed on the level of a service API, for example those of security processors . Here, valid commands are executed in unusual sequence, thereby provoking unintended behaviour in favour of the attacker. To our knowledge, the service (message) interfaces of sensor networks have not been investigated with regard to security vulnerabilities. Instead, most work has been done to secure the wireless interface. Attacks on the wireless interface of sensor nodes are easy to execute as they require only a wireless transceiver. Either an external device could be used, or captured nodes of the sensor network itself, after a successful physical attack on some of the nodes. There are some  difference is in the coverage of the deployment area: a high-powered external device may enable the attacker to reach all nodes at the same time, while single sensor nodes have a much more limited radio range. Some attacks on the transport layer can be thwarted easily.Other attacks are almost impossible to prevent, such as jamming. Some mitigation techniques are applicable, though. If only a limited region is affected, it may be possible to route around it. In hybrid networks , which employ additional wired connections, a jammed node could raise an alert outside the jammed region. A possibility for preventing jamming would be the use of directed optical instead of radio links, but those are much harder to deploy. The risk of an attack occurring on the wireless communication of a sensor network is quite high, since it is relatively easy to mount. The impact of such an attack can be mitigated by measures such as message encryption and authentication, and by reporting jamming attacks. Experience teaches that careful design and implementation of cryptographic mechanisms is necessary to ensure that the security goals are achieved. The vulnerabilities of link layer encryption in the IEEE 802.11 standard is a popular example . Much of the research work on the security in sensor networks, as described in the previous chapter, is concerned with the design of such mechanisms that are suitable for sensor networks.

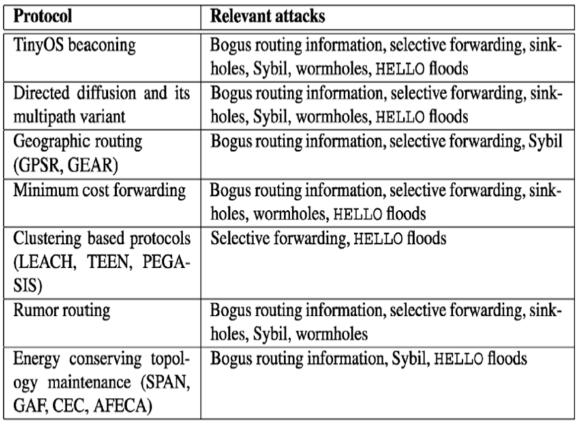
**Software-Level Attacks**
A powerful attack is the injection of code into an execution environment, since this yields potentially full control over this environment. Such attacks are common in the Internet world, where poorly administrated hosts are susceptible to adversarial remote control. One of the reasons for this is code mobility i.e. code is often downloaded from remote sites and locally executed. Even if mechanisms for code certification exist, these are often circumvented by social engineering or user inattentiveness. Sensor networks are comparatively more closed environments, but code updating is a common feature and introduces similar vulnerabilities.

Software for wireless sensor networks is often developed using low-level programming languages like C. This facilitates the introduction of vulnerabilities such as buffer overflows . Fortunately, microcontrollers (which are the basis for sensor nodes) are often based on the Harvard computer architecture, which physically separates program and data memory. In such an architecture, buffer overflows usually don't lead to unwanted program execution, since most programs don't write into program memory directly. However, moving to processors that are based on the von Neumann architecture, or using virtual machines exposes sensor networks to the risks of such vulnerabilities.

Custom software development can reduce the risk of software-level attacks,since the exploitation of vulnerabilities in such systems is more costly to an attacker than in standardized systems. Also, the absence of software lifecycle management mechanisms allows it to build such restricted interfaces that further reduce the risk of vulnerabilities. However, both approaches put harsh restrictions on the flexibility and the cost-effectiveness of such systems. It can therefore be safely assumed that a more open approach will be usually used in

**sensor networks in the future.**
In general, one can differentiate between primary and secondary objectives that an attacker pursues. The primary objectives concern the informational resources the attacker wants to gain control of. His goal may be to acquire some secret information, or disrupt a service, or falsify some data in order to hide the the presence of facts, just to mention some examples. The secondary objectives are concerned with the circumstances of an attack.

As we concluded that end-to-end mechanisms would be either too costly or too constraining in many applications of wireless sensor networks, we considered the approximation of end-to-end security as an alternative approach that provides a level of security that is sufficient for many purposes and may deter potential attackers in many cases.



| Protocol | Relevant attacks |
|---|---|
| TinyOS beaconing | Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods |
| Directed diffusion and its multipath variant | Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods |
| Geographic routing (GPSR, GEAR) | Bogus routing information, selective forwarding, Sybil |
| Minimum cost forwarding | Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods |
| Clustering based protocols (LEACH, TEEN, PEGASIS) | Selective forwarding, HELLO floods |
| Rumor routing | Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes |
| Energy conserving topology maintenance (SPAN, GAF, CEC, AFECA) | Bogus routing information, Sybil, HELLO floods |

**Fig.1.summary of attacks against proposed sensor networks routing protocols**

Security protocols are Secure Network Encryption Protocol (SNEP) which provides confidentiality, authentication and MicroTimed Efficient Stream Loss (μTESLA) provides authenticated broadcast. Secure Network Encryption Protocol (SNEP).

**CONVENTIONAL APROACH FOR SECURED DATA AGGRIGATION METHODS**
Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values.

**IF algorithms**
Identification of a new sophisticated collision attack against IF based reputation systems which reveals a severe vulnerability of IF algorithms.

A novel method for estimation of sensors errors which is effective in a wide range of sensor faults and not susceptible to the described attack.

Design of an efficient and robust aggregation method inspired by the MLE, which utilizes an estimate of the noise parameters, obtained using contribution 2 above.

Enhanced IF schemes able to protect against sophisticated collision attacks by providing an initial estimate of trustworthiness of sensors using inputs from contributions 2 and 3 above.

IF Scheme we implemented on HEF and TEEN protocol to analyze the simulation performance.

In addition to IF algorithm, High Energy First(HEF) algorithm is also used to change CH node in a region when it loses its energy

**HEF ALGORITHM**
High Energy First (HEF) is another efficient secured data aggregation method.

**Step I: Cluster Head(CH) Formation**
Initially all the nodes share message to all neighboring nodes.

All the nodes check their respective energy level with received energy level.

The node with higher energy will act as Cluster Head and intimate all other nodes that it is CH

**Step II: Start message from source to base station.**
If route exist in route table then check the energy consumption speed of CH. Else insert the message in queue.

Step III:If consumption speed is high then forward the message. Else changing of the CH takes place based on the value

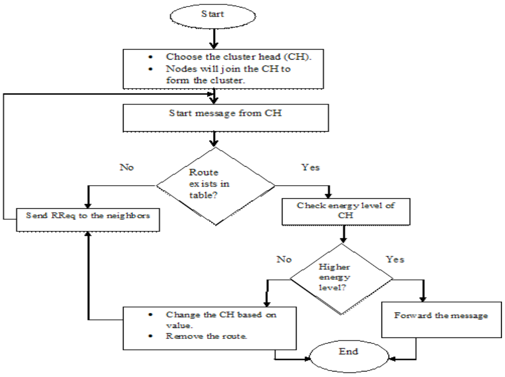


**Fig.1.2.HEF algoritham**

The number of nodes sends the data to the aggregator. The all the nodes have different types of data format. So to aggregate the data that is send to the aggregator node. The aggregator node is also a node that will process the above diagram. Calculate distance of nodes and its trust values. Trusted nodes only send data to cluster head. Based on the information in the packet the nodes trust value is calculated. In this aggregation process the node will sends the data to the aggregator. The aggregator compares the each and evergy data. That task is performed by the variance estimator. If the different is more over the data comes for the malicious node. Maximum same data are comes from the goog node. This is not a single time process.it is the iterative process. Based on this approach we can easily identify the trustable nodes by the data aggregation. So this is called secure data aggregation.

Secured Data Aggrigation using Filtering method(SDAF)

**Tree Model:**
Residual energy of the neighbor is accessed, high energy neighbor is selected as parent and it is attached with hello message

On receiving the hello message, the node checks its id and the parent id mentioned in the hello message. If it matches it adds the node that sent the hello message to its member list.

Each node is aware of child and its member list

**CH- Parent ,Member-child,Synopsis Diffusion**
Bitstring for every temperature data is computed for every sensor and transmitted to parent (CH)

Every sensor generates MAC for it using its genuine key

After all data are received by parent, it accesses the synopsis and corresponding MAC

OR operation of the received synopsis is computed by the parent

BS finds a sensor as attacker if its MAC is invalid and excludes corresponding data

BS verifies MAC for every received bit and if no valid MAC is found for a bit it discard the bit and broadcast control packet by querying valid MAC for the bit.

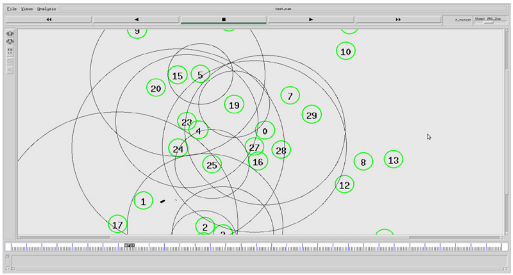
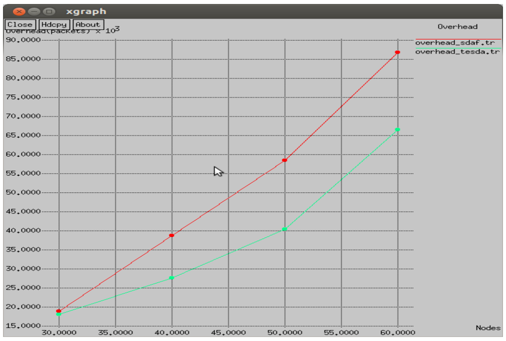


**Fig.1.***3. False Data Injection Attack by Parent*

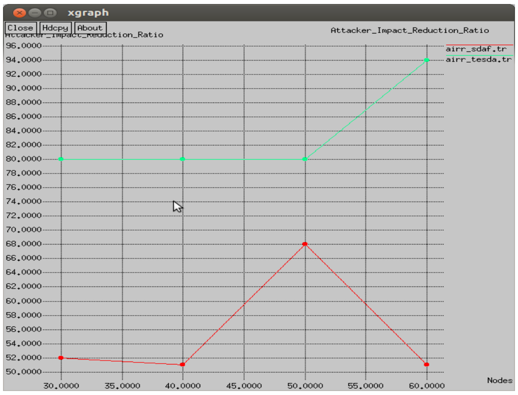
BS verifies received MAC and filters unauthenticated bit from final fused synopsis.

**RESULT**
**Comparison of TESDA and SDAF**
**Network lifetimeOverhead**



Overhead of SDAF is high when compared to TESDA because, SDAF incurs control packets for verification of MAC. In the case of invalid MAC it broadcast control packets for to fins valid MAC for the received bit which is not the case in TESDA.

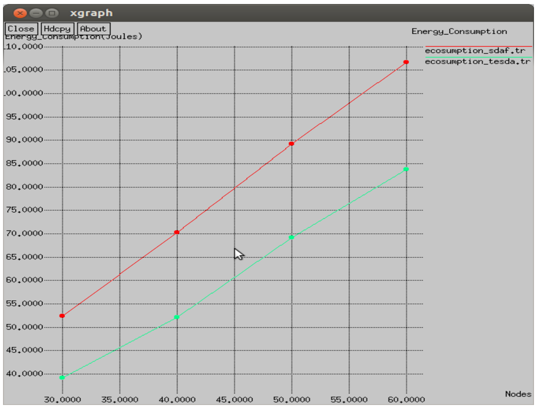
**Attacker Impact Reduction Ratio**



Volume : 6 | Issue : 9 | September 2016 | ISSN - 2249-555X | IF : 3.919 | IC Value : 74.50

Attack impact is reduced in TESDA when compared to SDAF because it takes the aggregation based on deviation but where as in SDAF, deviation is not considered for aggregation.

### Energy Consumption



Energy consumption is reduced in TESDA when compared to SDAF because of the reduced control packets involvement. It increases when the number of nodes are increased due to the increased overhead.

### Conclusion

Compared to all methods TESDA is more efficient secured data transmission technic.This method further improved by increasing no of nodes and more energy efficient.

### References

1. Roy, Sandip, et al., "Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact", IEEE Transactions on Information Forensics and Security, Vol.9, No.4, pp.681-694, 2014.
2. Zhu W, Xiang, Y & Zhou, J 2011, 'Secure localization with attack detection in wireless sensor networks', International Journal of Information Security, vol. 10, no. 3, pp. 155-171.
3. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
4. Pradeepa, K, Anne, WR & Duraisamy, S 2012,'Design and implementation issues of clustering in Wireless Sensor Networks', International Journal of Computer Applications, vol. 47, no. 11. pp. 23-
5. Kavitha, T & Sridharan, D 2010 'Security vulnerabilities in Wireless Sensor Networks: A survey', Journal of Information Assurance and Security, vol. 5, pp. 31-44.
6. Alcaraz, C, Lopez, J & Roman, R 2012, 'Selecting Key Management Schemes for Wireless Sensor Networks application', Journal of Computers and Security (Elsevier), vol. 31, no. 8, pp. 956-966.
7. Azarderskhsh, R & Reyhani, A 2011, 'Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks', Eurasip Journal on Wireless Communications and Networking, Article ID: 893592, pp. 1-12
8. Chan, AC & Castelluccia, C 2011, 'A security framework for privacy preserving data aggregation in wireless sensor networks', ACM Transactions on Sensor Networks (TOSN), vol. 7,no. 4, p. 29,
9. Chatterjea, S. and Havinga, P. "A Dynamic data aggregation scheme for Wireless Sensor Networks," in Proc. ProRISC, pp. 56-60, 2003.
10. Chee-Yee Chong & Kumar, P 2003, 'Sensor Network: Evolution, opportunities and Challenges', Proceeding of the IEEE 11th Internation Conference on Trust, Security and privacy in Computing and Communications, vol.91, no. 8, pp.1247-1256.
11. Lopez, J, Roman, R & Alcaraz, C 2009, 'Analysis of security threats, requirements, technologies and standards in Wireless Sensor Networks', Journal of Foundations of security analysis and design, vol. 5703, pp. 289-338.