A REVIEW OF MALICIOUS NODE DETECTION TECHNIQUES AND ENERGY EFFICIENCY CONSERVATION METHODS IN WIRELESS SENSOR NETWORK

N. Geetha Lakshmi [1], Dr.D.Shanmuga Priyaa[2]

ABSTRACT

The data transfer in Wireless Sensor Network is more prone to various kinds of attacks, as the nodes of the network are present in open, unprotected and hostile environment. It is more challenging to transfer data in such environment by preserving the security and lifetime of the network. The objective of the wireless sensor network is information gathering, monitoring and reporting; hence it is much necessary for the wireless sensor network to have a secured space for authenticated data transfer An efficient energy management also plays a vital role in determining the lifetime of a wireless sensor network. In general, the wireless sensor network is powered by a battery and it is tough to recharge. Therefore, extending the lifetime of sensors to enhance the network's performance is a major challenge in wireless sensor network. This paper aims to review various existing techniques used to find the malicious nodes in a wireless sensor network, along with the causes of energy loss and its conservation schemes.

Keyword : Wireless Sensor Network (WSN), Malicious Network, Compromised Nodes, Types of Attacks, Intruders, Energy conservation, Duty cycling and Energy efficiency.

I. INTRODUCTION

Wireless Sensor Network is an emerging technology which advances its vigorous application in various fields such as health care, logistics, Telematics, surveillance etc. The requirement of applications like fewer amounts of memory, lower energy consumption and small area of communications hikes the demand of wireless sensor network.

Wireless Sensor networks can be defined as a distributed network comprising a collection of inexpensive devices called sensor nodes which are connected to one another to work in coordination for the particular task of recognising the environment, processing of data and storing and transmission of sensed data through wireless channels (Akyildiz & Kasimoglu, 2004)[2].

The Wireless sensor network can be used either as a scheme with static sensors or portable nodes. This system is capable of sensing variations in temperature, vibration, humidity and other physical environmental conditions. These data are processed locally and the result is sent to the sinks. In this setup, every node in the network will be built-in with a battery of limited capacity, which is very difficult to change or recharge due to the kind of environment in which they are deployed (Papadinitrinou & Georgiadis, 2006)[16].

There are four main parts in every node of a Wireless Sensor Network. They are:

[1] Research Scholar, Dept.of Computer Science, Karpagam Academy of Higher Education, Coimbatore - 641 021

[2] Professor, Dept. of CS, CA& IT, Karpagam Academy of Higher Education, Coimbatore - 641 021

(i) Sensors to sense data to be acquired,

(ii) Processor along with in-built memory to process local data,

(iii) Communication hardware for wireless data communication; and

(iv) Power supply unit.

The base station (Sink Node) can also be referred to as a gateway with high processing power and memory space that receives the sensed data from each node, processes it and sends it to the outside wired world. The network does not involve any pre-described structure and no centralized controlling exists. The communication between sensors is within a limited transmission range using radio link, through either direct as peer to peer fashion or multihop strategy.

Basically, a wireless sensor network is amenable to a glut of intrusion due to its broadcasting nature of transmission. This feature gives the gap for an adversary to eavesdrop as the data transfer and fault data spreads across the network. Thus vulnerability in wireless network is higher than in a wired habitat. Hence, preserving the integrity and authentication of wireless sensor network is a burdensome and, of course, difficult. There are different types of attacks commonly referred to as active and passive. Active attacks are easier to detect since their effects can be easily monitored due to the changes occurring in the network and over its elements. On the other hand, passive attack accounts for a silent killing approach; it neither shows its presence nor can be easily detected. So it is more strenuous to capture it.

The lifespan of a sensor network can be enhanced by using different techniques. The minimal energy consumption can be achieved by using energy efficient protocols. A significant amount of energy consumption happens through other components like CPU, Radio etc., as they consume energy even in their idle state. (Dimirkol, et al. 2006)[11]. Therefore, various power-monitoring schemes are implemented so as to switch-off the components when they are not used.

(S. Rajasegarar et al,2008)[19]. show an overview of various existing anomaly detection schemes in wireless sensor networks and describe two approaches for intrusion detection. The first approach is misuse or signature based detection, where the signature of known attack is stored and compared with the monitored attack. The second approach is anomaly detection where deviation in the behaviour of monitored data is checked to detect an attack. Anomaly detection is categorized into statistical and non-parametric techniques. Statistical techniques are application dependent and are used when prior knowledge about data distribution is available. While non-parametric is used where there is dynamic data distribution without any prior knowledge.

Padmavathy et al, 2009[15] conducted survey deals with different attacks and their eff G.ects in wireless sensor networks. They also describe various challenges faced by WSN. They illustrate some of the techniques for detection of malicious activities in wireless sensor networks along with the analysis of energy conservation techniques carried out. They emphasize three major concepts: duty cycling, data reduction and mobility.

2. Existing Techniques to Detect Malicious Behaviour/Nodes in Wireless Sensor Networks :

A. Neighbor based malicious node detection in Wireless Sensor Networks

(Sung-Jib Yim et al)[20]. proposed a system where he explained a neighbour node based malicious detection system. Here malicious nodes meant, those nodes which generated wrong decisions by behaving like regular normal noYdes. Hence each decision making process was done through the wrong readings from itself and neighbours.

Fault in a network can be transitory, but this fault will be responsible for incorrect readings and performance loss or permanent fault or unreliability in network. Transitory fault could occur often and smoothing filters were used to remove it where it avoided unnecessary alarms in event driven detection. Permanent fault could be detected using confidence level evaluation as each node maintained confidence level of its own and its neighbours and evaluated trustworthiness between them. After each periodic and event driven cycles each node updated its own confidence level and also its neighbours' for further decision making. Updating procedure was done through two parameters, which could differentiate malicious nodes from normal nodes by observing their behaviour.

B. Usage of Auto regression Technique to identify Mischievous Nodes in Wireless Sensor Networks

Malicious detection through a time series evolution of sensor data was presented by (D. I. Curiac et al.)[7] Initially every sensor node was assigned a threshold value depending on its type. Malicious sensor node was detected by comparing the value provided by the sensor node at the moment with the predicted output value which was obtained from the past/present values of the same sensor through an auto regressive predictor. If the comparison showed a high difference from threshold value, the node was considered malicious and decision block was activated. A case study was also described to show the effectiveness of this method.

C. Cluster-based Reputation and Trust for Wireless Sensor Networks

G. V Crosby et al.[22] proposed a unique approach for preventing the selection of compromised or malicious cluster heads. A secure cluster formation algorithm was developed to launch the trusted cluster through pre-distributed keys. After the development of the cluster, whenever the existing cluster head's power failed, a new cluster head was selected by passing new cluster election message to cluster members. Through a voting approach from these members a new candidate with top ranked trust value from trusted neighbours list was chosen as new cluster head. Before being launched as cluster head it underwent a challenge - response stage with current cluster head. If it passed the test, it was selected; else it was moved to blacklist and its trust level set to -1.Once a sensor node's trust value was set to -1 it implied that there was no trust level updation or any further relation with that node. The experimental analysis of this algorithm concluded that, this approach reduced the chances of making compromised nodes as cluster head.

D. Distributed Reputation-based Beacon Trust System (DRBTS) :

A novel distributed security protocol that enhanced ideal nodes to monitor one another in order to detect erroneous location information from malicious beacon nodes was proposed by (Azna Asharaf, 2018) [1] The beacon nodes were mainly placed to assist sensor node for location initialization. Here each beacon node used second hand information for maintaining reputation of nodes, after passing through a deviation test. Every beacon node monitored its neighbour nodes to identify mischievous beacon nodes and accordingly updated the reputation of that node in the neighbour-reputation table. This table was used by each sensor node to determine whether or not to use the location information of corresponding beacon node using a majority voting approach. DRBTS utilized first and second hand information to maintain the trust in a network.

E. An Intrusion Detection Technique Based on Weighted Trust Evaluation for Wireless Sensor Networks

(Azna Asharaf, 2018) [1]. proposed a weighted-trust application (WTA) technique to identify the compromised nodes from reporting false data and preventing sink nodes from accepting it. The mechanism in this scheme was to assign each sensor node a weight value ranging from 0 and 1. Weight value would act as an interface to the sink node, be mainly placed to improve reliability and trust. Initially the value was 1 and went on changing in every cycle, depending on the node's performance. A node was identified to be malicious if the weighted value fell below a threshold value and a more precise aggregation result could be obtained by comparing node's weight sum value. The simulation results of this approach showed robustness on different sizes of network.

F. An analysis of the Elimination of False Malicious Node Detection using Watchdog Mechanism in Wireless Sensor Network

(Jijeesh Baburajan et a,2014l)[12]. proposed a paper showing the confines of watchdog mechanism and the countermeasures to overcome them. Watchdog was an intrusion detection mechanism in a wireless sensor network which monitored the malicious nodes from their misbehaviour during every transmission. The mechanism involved nodes as watchdogs, which might eavesdrop on the message between other nodes and decide whether to discard or forward it. This occurred mainly because of the broadcast nature of the wireless sensor network.

The main limitations reviewed were Ambiguous collision, Receiver collision, Limited transmission power, false misbehaviour detection and partial dropping. This problem could be overcome through an improved version of watchdog technique.

G. An improved watchdog technique established on power-aware hierarchical design for ids in wireless sensor networks

To preserve security and networks' lifetime by removing the limitations in an ordinary watchdog mechanism, an improved version was implemented by A.Forootaninia et al.[10] It was a power aware hierarchical model where, the cluster head node would act as a watchdog and execute the operation. For effectiveness the mode l was simulated using TinyOS simulator and compared with non-hierarchical model.

The work defined the hierarchical design based intrusion detection system and comparison of ordinary Watchdog with improved mechanism. The result showed that though the ambiguous collision was not resolved, the majority of snags in ordinary watchdogs were fixed in this upgraded technique.

H. Dual Threshold technique to detect Malicious Node in Wireless Sensor Networks

(SungYul.Lim,etal,2013)[21] suggested an advanced form of malicious node detection through dual threshold structure, mostly applicable in fault prone network rather than single threshold. The first threshold endorsed event detection thereby reducing false alarm rates. The second threshold made event nodes pass the test, and later the exact event region was detected accurately. To overcome the instability between the nodes each node possessed a trust value along with threshold values for decision making.

3. Energy Conservation Techniques

Energy is the most significant resource for wireless sensor network. But the common problem in wsn is the absence of consistent power for each sensor node in the network. Within a network, breakdown of the energy consumption depends on the specific sensor node. Several trials have shown that, the cost of a single bit of information transmission is same as the one required to process a thousand operations (Raghunathan et al. 2002)[18]. In gist, transmission of data consumes much more energy than processing of data.

Though, in the sensing subsystems the consumption of energy by every node varies, in some cases, energy consumption is less for sensing, than data processing, while in others the energy consumption is more for sensing than processing.

Many studies were done to resolve the above problem, and it has resulted in different techniques and protocols. Most of these power conservation techniques focus on sensing and networking subsystems. Therefore, both energy efficient protocols (wherein network activities consume minimal energy) and power management schemes(wherein node components are switched off when idle) are essential for minimum energy consumption in wireless sensor networks (Pottie and Kaiser, 2002)[16]. The above schemes and protocols are grouped as :

3.1 Duty-cycling

3.2 Data reduction

3.3 Mobility

In this article, first two are analysed. Each of these schemes is further divided into several parts.

3.1 Duty Cycling

The sensor node radio operation has two modes: Active Mode and Sleep Mode. Depending on the activities the sensor nodes in the sensing subsystems and swing between modes, this behaviour of a node is known as Duty Cycling (Lai, 2010)[13]. It is observed that, in wireless sensor network, during the idle mode, idle energy is very significant in saving energy.

Thus, Duty cycle is the percentage of time a node is active during its lifetime. Using the following two approaches, Duty cycling can be efficiently implemented.

The first approach is called "Topology Control". This method uses a minimum number of nodes to forward and route data packets generated by other nodes, without affecting the network periphery and connectivity. Here, the network longevity is prolonged, as this system ensures that nodes not currently in use will go to sleep and save energy. This scheme has been designed and analysed by Warrier et al (2007)[23]. This scheme is similar to the existing protocols, but differs in defining the rule of thumb, which determines the obtainable energy gain in the given density of network. This technique was implemented on a 42 node mica2 test bed. This implementation yielded nearly two times energy gain.

The second approach is termed as "Power management scheme". Under this scheme, MAC protocols and a wakeup scheduling scheme are introduced, so that a node sleeps when it is in idle state and still maintains network connectivity, but the usage of other resources are minimal. TRAMA, BMAC and ZMAC are some of the low duty cycle MAC protocols. The TRAMA is a Time Division Multiple Access (TDMA) scheme; here the energy consumption is significantly reduced as the nodes converse only during their assigned slots. BMAC is a contention based protocol, here low power communication is achieved through low power listening. In this scheme, each node has an independent awake and sleep schedule and utilizes low power communication during that period. ZMAC, a hybrid protocol incorporates the behaviours of both contention-based scheme and TDMA scheme, depending on the network's level of contention. If the contention level is high, TDMA scheme is employed and if the contention level is low, contention-based protocol is used. (Demirkol et al. 2006)[11].

Lai (2010)[13] found three categories of neighbour discovery mechanism to achieve the wakeup scheduling:

- On-demand wakeup
- Scheduled neighbour discovery
- Asynchronous neighbour discovery

● **"On-demand wakeup" mechanism :**

In this mechanism, sleeping nodes are woken on need. This means that a node will be woken up only when another node is ready for communication with it. But, the challenge lies in informing the sleeping node about another node which is ready and wants to communicate. This can be resolved by using multiple radios with different energy trade-offs. The results have shown that this scheme is highly energy efficient.

● **"Scheduled wakeup" mechanism:** Here, sleeping nodes wake up simultaneously in their stipulated wake-up schedule, communicate with one another and then go back to sleep mode till their next wake-up schedule. S-MAC and the multi-parent schemes protocols use this scheme of wakeup.

● **"Asynchronous wakeup" mechanism:** This mechanism does not need clock-synchronization, as scheduled wakeup is not used. In this scheme, a node can wake up any time and can communicate with the other nodes. This has many advantages over other schemes, such as ease of implementation along with low message overhead for communication.

3.2 Data Driven Approach :

In this approach, energy consumption is reduced in two ways (Arunraja&Malatha, 2012)[5]: In the first step, energy consumption is reduced by categorising the unnecessary samples and restraining them from being transmitted to sink. In the Second step, the accuracy of the sensor is kept at a reasonable level, so that the power consumption of the sensing subsystem is reduced. Through the first step, the problem of unnecessary sample transmission is solved and by implementing the second step, power spent on the sensing subsystem is reduced.

Data-driven approaches can be implemented using two schemes: Data-reduction schemes and Energy-efficient data acquisition schemes (Anastasi et al., 2009)[4].This classification is as per the problems they encounter.

3.2.1 Data-reduction schemes : Here, three different techniques are used to curtail the quantity of data transmission to the sink node. They are:

- In- networking processing
- Data compression
- Data prediction.

In-network processing: Here, Data aggregation is done at intermediary nodes to reduce the quantity of data transmission from source to sink (base station). It is observed that this technique is good when accurate reading is not significant and readings of the sensors are not dynamic (Zhang, 2012)[28].

Data compression: Here, to reduce the amount of data transmission, information encoding is done at the source nodes and the decoding of the same is done at base station.

Data Prediction: In this technique, data prediction is done at both source and sink nodes using adaptive filters.

Zhang (2012)[28] proposed an aggressive data reduction algorithm based on error inference within sensor segments. This system combined three kinds of error control mechanisms, to achieve both data validity and energy savings. The performance assessment of this algorithm was done through an experiment using a readily available soil temperature data. The outcome showed that the proposed algorithm produced up to 50% more energy saving than several existing sensing schemes.

3.2.2 Energy-efficient Data Acquisition Scheme :

This technique focuses on high - reduction of radio energy consumption rather than energy consumption by sensing subsystems (Alippi et al., 2009)[3]. Here the aim is to reduce data samples which in turn reduces the number of communications. This scheme can be further classified into three types. They are:

Hierarchical sampling

Adaptive sampling

Model based sampling

- The hierarchical sampling approach: Here, every node is fitted with many types of sensors and each sensor is chracterized by its own accuracy and its relative energy consumption. This technique takes dynamic decisions, activates the respective classes when there is a trade-off between power conservation and accuracy.
- Adaptive sampling technique: In this technique, similarities amongst the sensed data are found so that the amount of data to be acquired from the transducer can be reduced. This is done in proportion to the available energy.
- Model-based active sampling: Here, a sensed phenomenon model is constructed based on the sample data, so as to predict the next data. This scheme reduces the amount of data being transmitted to the sink, by exploiting the obtained model to reduce the number of data samples..

Chen & Wassell (2012)[8], has proposed a data acquisition scheme, in which the count of samples acquired by the sensor nodes are minimized, by using the theory called compressing sensing theory. This new framework of random sampling scheme considers the interconnection of sampling data, their hardware limitations and the balance between the randomization scheme and computational complexity. This framework has a scheme for sampling rate, which allows the sensor to adjust the rate at which it samples data and maintains a realistic performance. Using real data collected by a WSN, the performance evaluation of this scheme is done. The results show that this scheme has the capability to greatly reduce the number of required samples, consequently reducing energy required for sampling & transmission.

4. Conclusion

The demand of WSN is high with emerging technologies, and so is its security. This article has surveyed some of the malicious node detection techniques for WSN. In this paper, malicious node detection techniques and the methods to resolve them are briefly outlined. This can be summarized to say that a node can be malicious if it is:

- Faulty and produces wrong data.
- There are fluctuations in the predicted & threshold value.
- Providing false report on data transmission.

Along with the above survey, the main approaches to energy conservation in wireless sensor networks are reviewed. The research works carried out to address this issue have proposed many schemes as well as protocols; a few of them are discussed here. It should be noted that most of these schemes/protocols forfeited one or more things in order to save energy. In data reduction algorithm there is a compromise between power saving and validity of data. The topology control approach neglects throughput to increase power saving. These drawbacks need to be resolved to increase the efficiency of the schemes. The other areas include energy garnering from the environment; it is not just a source of energy but also a means of energy conservation in wireless sensor networks.

References :

1. Azna Asharaf (2018) "Techniques for Malicious Node Detection in Wireless Sensor Networks - A Survey" IJSRD - International Journal for Scientific Research & Development| Vol. 6, Issue 03, 2018 | ISSN (online): 2321-0613

2. Akyildiz I. F. & Kasimoglu I. H. (2004) "Wireless Sensor and Actor Networks: Research Challenges", Ad Hoc Networks Journal, Vol. 2, No. 4, pp. 351-367,.

3. Alippi C., Anastasi G., Francesco M.D. & Roveri M. (2009) "Energy Management in Wireless Sensor Networks with Energy-hungry Sensors" IEEE Instrumentation and Measurement Magazine Vol. 12, N. 2, pp. 16-23

4. Anastasi G., Coti M., Frrancesco M. & Passarella A.(2009), "Energy Conservation in Wireless Sensor Networks:A Survey", Elsever, Ad Hoc Network,.

5. Arun-raja M. &Malathi V.(2012) "An LMS Based Data Reduction Technique for Energy Conservation inWireless Sensor Network" Int.J.Computer Technology &Applications, Vol 3 (4), 1569-1576 IJCTA | pp 1569-1576.

6. Bolaji Omodunbi, O.T. Arulogun J.O. Emuoyibofarhe "A Review of Energy Conservation in Wireless Sensor Networks "Network and Complex Systems, Vol.3, No.5, 2013 ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)

7. D. I. Curiac, O. Baniavinashas, F. Dragan, C. Volosencu and O.Dranga, "Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique," 3rd International Conference on Networking and Services, Athens, 19-25 June 2007, p. 83..

8. Chen W. & Wassell I.J. (2012), "Energy Efficient Signal Acquisition in Wireless Sensor Networks : A Compressive Sensing Framework" Wireless Sensor Systems, IET ,Volume:2 , Issue: 1, pp 1-8

9. Demirkol I., Ersoy C., &Alagöz F. (2006), "MAC Protocols for Wireless Sensor Networks: A Survey" IEEECommunications Magazine, pp 115 - 121.

10. Forootaninia, M. B. Ghaznavi-Ghoushchi, "An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS In Wireless Sensor Networks", International Journal of Network Security & Its Applications (IJNSA), 2012..

11. Jain S., Shah R. , Brunette W., Borriello G. & Roy S. (2006), "Exploiting Mobility for Energy Efficient Data Collection in Wireless Sensor Networks", ACM/Springer Mobile Networks and Applications, Vol. 11, pp. 327-339.

12. Jijeesh Baburajan, Jignesh Prajapati, "A Review Paper On Watchdog Mechanism In Wireless Sensor Network To Eliminate False Malicious Node Detection", Volume: 03 Issue: 01 , Jan-2014

13. Lai S. (2010), "Duty-Cycled Wireless Sensor Networks: Wakeup Scheduling, Routing, and Broadcasting" a thesis submitted to Virginia Polytechnic Institute and State University,.

14. Luo J &Hubaux J.P.(2005), "Joint Mobility and Routing for Lifetime Elongation in Wireless Sensor Networks", Proc. IEEE Infocom 2005, vol. 3, pp. 1735-1746, Miami (USA).

15. G. Padmavathy, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," International Journal of Computer Science and Information Security, IJCSIS, Vol. 4, No. 1 & 2, August 2009.

16. Papadimitriou I. & Georgiadis L. (2006) "Energy-aware Routing to Maximize Lifetime in Wireless Sensor Networks with Mobile Sink", Journal of Communications Software and Systems, Vol. 2, No. 2, pp. 141-151, June 2006.

17. Pottie G, Kaiser W, (2000), "Wireless Integrated Network Sensors, Communication of ACM, Vol. 43, N. 5, pp.51-58.

18. Raghunathan V., Schurghers C., Park S., Srivastava M.(2002), "Energy-aware Wireless MicrosensorNetworks",IEEE Signal Processing Magazine, pp. 40-50.

19. S. Rajasegarar, C. Leckie and M. Palaniswami, "Anomaly Detection in Wireless Sensor Networks," IEEE Wireless Communications, Vol. 15, No. 4, 2008, pp. 34-40.

20. Sung-Jib Yim, Yoon-Hwa Choi, "Neighbor-Based Malicious Node Detection in Wireless Sensor Networks" Vol.4 No.9(2012), Article ID:22509,in Scientific Reasearch, September 2012.

21. SungYul,Lim and YoonHwaCho, "Malicious Node Detection Using a Dual Threshold in Wireless Sensor Networks", J. Sens. Actuator Netw. 2013,2,70-84; doi:10.3390/jsan201007, 5 February 2013.

22. G. VCrosby and Niki Pissinou, "Cluster based Reputation and Trust for Wireless Sensor Networks", in the proceedings of the IEEE Consumer Communications and Networking Conference, January2007.

23. Warrier A., Park S, Min J. & Rhee I. (2007), "How much energy saving does topology control offer for Wireless Sensor Networks" Comput. Commun.i:10.1016/j.comcom.2007.05.019.

24. Ye W. &Heidemann J. (2003) "Medium Access Control in Wireless Sensor Networks" Technical Report ISITR- 580, USC/Information Sciences Institute.

25. Yun Y. & Xia Y. (2010), "Maximizing the Lifetime of Wireless Sensor Networks with Mobile Sink in Delay- Tolerant Applications" Mobile Computing, IEEE Transactions Volume:9 , Issue: 9 pp 1308 - 1318.

26. Zhang Q.(2012), "Cooperative Data Reduction in Wireless Sensor Network" Globecom 2012- Adhoc and Sensor Networking Symposium, pp 646-651.

27. Zhao W., Ammar M., &Zegura E.(2004), "A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks", Proc. of ACM MobiHoc 2004, Tokyo (Japan).