International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Revised Approach on Attack Identification and Handling in WSN

Seema Khokher[1]

[1]MERI College of Engineering & Technology, Sampla (Haryana), India

Abstract: ***Security is one of the most critical vectors for any network. When the network is an open adhoc network, this criticality also increases. Sensor network is one of such network that suffers from different kind of internal and external attacks. The internal attacks are more crucial for the network because it is done by the authenticated member nodes. These attacks affect the network by affecting the QoS parameters over the network. In this present, a layered architecture is presented to handle the internal attack in wireless sensor network and to provide the effective throughput over the network. The presented work is divided in three stages. In first stage, the network nodes are analyzed under the throughput, delay and energy consumption parameters. Based on this analysis, the first level critical nodes are identified. Now before deciding the nodes as the attacker nodes, these nodes are required to keep in observation. At the second stage, to observe the nodes, the effective monitoring node selection is defined in this work. To monitor each attacker nodes m observer nodes are identified under the coverage range and energy parameters. The analysis on these nodes is performed under different parameters such as PDR, energy loss, communication delay etc. Now at the third stage, the Dempster-Shafer theory will be applied on this parameteric evidence under different beliefs. Based on these belief oriented observation, the identification of the attacker node will be done..***

Keywords: WSN Characteristic parameters, Dampster Shafer Theory, Attacker, Energy consumption

1. Introduction

Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances. These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. These sensor nodes can sense, measure, and gather information from the environment and, based on some local decision process, they can transmit the sensed data to the user.

A sensor is a device that measures a physical quantity of signals and converts it into a voltage or current, analog or digital signal which can be read by an observer, instrument or by an computer (microcontroller) based instrument. Sensors are used in everyday objects. Wireless Sensor Device has 6 main parts Sensors, I/O interface, Memory, Processor, Radio and Battery. A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure properties of the environment. Since the sensor nodes have limited memory and are typically deployed in difficult-to-access locations, a radio is implemented for wireless communication to transfer the data to a base station. Battery is the main power source in a sensor node.

Wireless Sensor Networks (WSNs) are self-configured and are without infrastructures. WSN collects data from the environment and sends it to a destination site where the data can be observed, memorized and analyzed. Wireless sensor devices responds to a “control site” on specific requests, or can be equipped with actuators to realize commands.

There are two types of WSNs: structured and unstructured. An unstructured WSN is one that contains a dense collection of sensor nodes. In a structured WSN, all or some of the sensor nodes are deployed in a pre-planned manner .Sensor networks represent a significant improvement over traditional sensors, which are deployed in the following two ways:

Sensors can be positioned far from the actual phenomenon. Several sensors that perform only sensing can be deployed A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it.

Unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

Some of the application areas are health, military, and security. For example, the physiological data about a patient can be monitored remotely by a doctor. Sensor networks can also be used to detect foreign chemical agents in the air and the water. They can help to identify the type, concentration, and location of pollutants. In essence, sensor networks will provide the end user with intelligence and a better understanding of the environment. Some other commercial applications include managing inventory, monitoring product quality and monitoring disastrous areas.

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions. In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery.

1. Classification of Sensor

Sensor can be classified on the basis of different aspects, including technological aspects, detection means, their output signals and sensor materials and field of application.

a) **Active Sensors:** Active sensors stimulate the environment in order to do the measurements. For example seismic sensors, laser scanners, infrared sensors, sonar's and so on.
b) **Passive, Directional Sensors:** These sensors can monitor the environment without disturbing the environment. Examples of these sensors are: thermometers, humidity sensors, light sensors and pressure sensors etc.
c) **Narrow Beam Sensors (Passive):** This is the type of passive sensors requires a clear direction in order to measure the environment (medium) e.g. camera and ultrasonic sensors.

2. Sensor Node Components

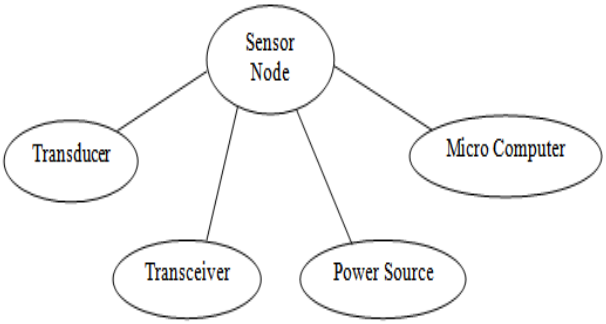

Figure 1: Components of Sensor Network

a) **Transducer:** Generates electrical signals based on sensed physical effects and phenomena. Micro-computer: Processes the sensed information and stores the sensor output.
b) **Transceiver:** Which can be hard wired or wireless. It receives commands from a central computer and transmits data to that computer.
c) **Power-source:** Derived from electric utility or battery. In most sensor networks, sensor nodes are homogeneous tiny devices with constrained energy supply and computational capabilities. In addition, we assume that all sensor nodes are stationary. The following characteristics of sensor nodes may differ for some networks. Hence, they can influence the protocol operation.
d) **Deployment:** Sensor nodes can be deployed in either a deterministic or a random fashion. When the nodes are deployed along a road-side, or in a metro-station, the deployment is rather deterministic than random.
e) **Transmission power:** The transmission power can be either dynamically adjustable or fixed. In the latter case, each sensor node transmits each message using the same energy level. In the former case, every node can calculate what energy level should be used to transmit a message to a neighboring node. This energy level may be inversely proportional to the cost assigned to the neighboring node.
f) **Coverage:** It is commonly assumed that a sensor node cannot reach all nodes in the network field. A routing protocol can require large transmission power per node in order to get a fully connected network. However, it can only be beneficial in small-sized networks due to the large energy consumption and interference range.
g) **Addressing:** The task of routing in sensor networks is to deliver the queries coming from the base station to the sensor nodes which have the requested data (in case of query-driven routing protocols, see later), and to return the requested data to the base station.
h) **MAC interface:** The data-link layer can be responsible for neighbor discovery (where the neighbor definition is protocol-dependent). In addition, it also needs to perform the calculation of cost values (where the cost definition is also protocol-dependent). Some routing protocols are integrated with the data-link layer in order to achieve better performance in terms network delay and energy consumption (cross layer design).

2. Proposed Work

In this present work an effective three stage model is been defined to identify the internal attack over the network. The presented work does not required any extra infrastructure for the analysis. The work is based on the evidence analysis on expected attacker node by different coordinating nodes. The evidences collected by these observer nodes will be analyzed using the belief metrics under Dempster-Shafer theory. Based on this analysis, the attacker node will be identified.

Stage 1: Level 1 Attack identification

At the earlier stage, the network nodes will be analyzed under different parameters to identify the attacker nodes over the network. These attacker nodes will be analyzed under different parameters such as energy, throughput and the delay. Based on the abnormal communication analysis, the expected attacker will be identified.

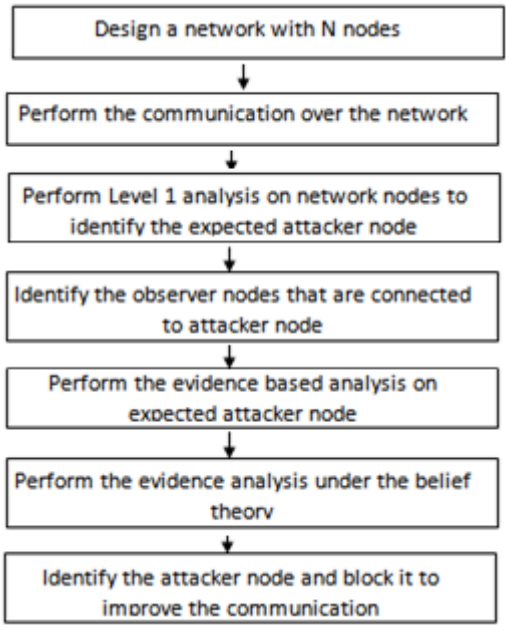

Figure 2: Attacker identification

State 2: Identification of monitoring nodes
At second level, the network nodes will be analyzed to identify the observer nodes over the network. The observer nodes will observe the expected attacker node under different

parameters. The observer nodes will be identified based on the energy and the coverage range analysis.

Stage 3: Dempster-Shafer theory
The observer nodes will perform the evidence information analysis on the attacker node under different parameters and the beliefs. These beliefs will be collectively used to generate the rule for the attacker node. Based on the evidence observation of these observer nodes the attacker node will be recognized.

3. Conclusion

Many researchers are currently engaged in developing the technologies needed for different layers of the sensor networks protocol stack. A major benefit of these systems is that they perform in-network processing to reduce large streams of raw data into useful aggregated information. Protecting it all is critical. Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly.

First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack.

And third, sensor networks interact closely with their physical environments and with people, posing new security problems. Consequently, existing security mechanisms are inadequate, and new ideas are needed.

A lot of work has been done for attacker node identification using rule based malicious node detection scheme, Markov Chain based anomaly detection algorithm, ACK based anomaly detection algorithm etc. But in the present work ,critical nodes are identified after analysis of the complete network on the basis of throughput, delay and energy consumption .Constant monitoring is kept over the critical nodes to identify one of the attacker node using DS theoretical concept. Finally , the attacker node is skipped for the communication after successfully evaluation of attacker node .In this work we add the concept of analysis of observer nodes with PDR, energy loss, communication delay etc.We consider the properties of a sensor network for the evaluation of network rather than any other complex techniques like anomaly finding methods using cryptographic algorithms.

4. Future Scope

Our current understanding of privacy in sensor networks is immature, and more research is needed. In our work, the attacker node is identified as it reflect a noticeable change in its energy, PDR, delay in the network. In future, this work could be enhanced to implement the algorithm in the hardware level to test in real time applications of data transfer. Secondly, network layering threats such as jamming and tampering in physical layer, collision, exhaustion, unfairness in link layer, spoofed, altered or replays routing information, selective forwarding, sinkhole and wormhole in network layer, flooding and de-synchronization in transport layer. Our work can be further extended to satisfy these different security levels.

References

[1] SuatOzdemir, Member, IEEE, and HasanÇam, Senior Member, IEEE,: “Literature survey Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks”, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 18, NO. 3, JUNE 2010
[2] Ling-Yi SUN, Wei CAI, Xian-Xiang HUANG Xi'an Research Inst of Hi-tech, Xi’an, China. “Data aggregation scheme using neural networks in wireless sensor networks”, IEEE: 978-1-4244-5824-0_c 2010]
[3] Ahmad Hosseingholizadeh ,Dr.AbdolrezaAbhari Department of Computer Science Ryerson University Toronto, Canada: “A neural network approach for Wireless sensor network power management”
[4] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci :” Wireless sensor networks: a survey”, Computer Networks 38 (2002) 393–422
[5] Ajay Jangra, priyanka, Swati, richa Wireless Sensor Network (WSN): A”rchitectural Design issues and Challenges”, (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 3089-309
[6] Shio Kumar Singh1, M P Singh, and D K Singh:” Routing Protocols in Wireless Sensor Networks” –A Survey, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010
[7] Shio Kumar Singh, M. P. Singh D. K. Singh: “ Applications, Classifications, and Selections of Energy-Efficient Routing Protocols for Wireless Sensor Networks”, (IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES Vol No. 1, Issue No. 2, 085 – 095
[8] KiranMaraiya, Kamal Kant, Nitin :Wireless Sensor Network:” A Review on Data Aggregation” ,International Journal of Scientific & Engineering Research Volume 2, Issue 4, April -2011 1 ISSN 2229-5518 ,IJSER © 2011
[9] Mohamed Watfa , William Daher and Hisham Al Azar :”A Sensor Network Data Aggregation Technique” ,International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009 1793-8201
[10] changlei Liu and Guohong Cao Department of Computer Science & Engineering The Pennsylvania State University : “Distributed Monitoring and Aggregation in Wireless Sensor Networks9”
[11] Sanjeev SETIA a,SankardasROYb and Sushil JAJODIA b a Computer Science Department, George Mason University, Fairfax, VA, USA b Center for Secure Information 10Systems, “Secure Data Aggregation in Wireless Sensor Networks”
[12] Roberto Di Pietro,Largo S. Murialdo, 00146 Roma, Italy ,PietroMichiardiRefikMolva “Confidentiality and Integrity for Data Aggregation in WSN Using Peer Monitoring “Antipoliscedex, FranceResearch Report RR-07-193,,16-04-200716

[13] Claude Castellucia, EinarMykletun, Gene Tsudnik, RefikHadzialic : "Efficient Aggregation of encrypted data in Wireless Sensor Networks" ,January 30,2007,
[14] Gerhard M¨unz, Georg Carle Computer Networks and Internet Wilhelm Schickard Institute for Computer Science University of Tuebingen, Germany : "Real-time Analysis of Flow Data for Network Attack Detection"
[15] Yong-Sik Choi*, Young-Jun Jeon*, Sang-Hyun Park,Dept. of Computer Science & Engineering, University of Incheon, 12-1 SongDo-Dong, Yeons-Gu, Incheon, South Korea : "A study on sensor nodes attestation protocol in a Wireless Sensor Network" ,ISBN 978-89-5519-146-2 - 574- Feb. 7-10, 2010 ICACT 2010
[16] Jianmin Chen and Jie Wu : "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks".NSF grants ANI 0073736, EIA 0130806, CCR 0329741, CNS 0422762, CNS 0434533, CNS 0531410, and CNS 0626240
[17] M. Pulido, P. Melin, O. Castillo : "Genetic Optimization of Ensemble Neural Networks for Complex" ,Time Series PredicProceedings of International Joint Conference on Neural Networks, San Jose, California, USA, July 31 – August 5, 201tion
[18] Neda Enami1, Reza Askari Moghadam1, Kourosh Dadashtabar2 &MojtabaHoseini "NEURAL NETWORK BASED ENERGY EFFICIENCY IN WIRELESS SENSOR NETWORKS": A SURVEY: International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010 DOI : 10.5121/ijcses.2010.1104 39
[19] Frank Yeong-Sung Lin," A Novel Energy-Efficient MAC Aware Data Aggregation Routing in Wireless Sensor Networks", Sensors 2009 ISSN 1424-8220
[20] Lei Zhang," Preserving privacy against external and internal threats in WSN data aggregation".
[21] Shih-I Huang," Secure encrypted-data aggregation for wireless sensor networks". Dirk WESTHOFF," Security Solutions for Wireless Sensor Networks".
[22] Claude Castellucia," Efficient Aggregation of encrypted data in Wireless Sensor Networks", WS 2009
[23] Steffen Peter," On Concealed Data Aggregation for WSNs".
[24] M.Y. Mohamed Yacoab," A COST EFFECTIVE COMPRESSIVE DATA AGGREGATION TECHNIQUE FOR WIRELESS SENSOR NETWORKS", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)
[25] V. Bhoopathy," Energy Efficient Secure Data Aggregation Protocol for Wireless Sensor Networks", European Journal of Scientific Research ISSN 1450-216X
[26] XiaoHua Xu," Efficient Data Aggregation in Multi-hop WSNs".
[27] Elhadi Shakshuki," P2P Multi-agent Data Transfer and Aggregation in Wireless Sensor Networks".

Author Profile

Seema Khokher has completed MCA from MDU in 2010 and now pursuing M. Tech from MERI College of Engineering and Technology.