Sensor Network Security algorithm based on Evidence theory

Sachika ,
Student ,MDU/ MERI College Sampla,Jhajjar ,
Haryana , India

Pramod Kumar,
Asstt. Professor Computer Science,
MDU/Nehru College, Jhajjar, Haryana, India

Pooja Khokher
Computer Science, Govt. College ,Dujana ,Jhajjar,

Haryana, India

Abstract— WSN i.e. Wireless sensor network are having low cost & multi functional resources and nodes with sensors to receive & transmit the data throughout the network .These nodes are very critical to the environmental situations .Incase of very sensitive applications the matter of security is at the peak as these type of network deals with a maximum factor of interaction through network .Hence, very much sensitive to both type of attacks: external & internal .Internal attacks are more crucial in this case as we have to make interaction with the network information again & again in which that malicious node is participating every time , that is the reason ,it needs hard efforts to identify the suspicious node .One more reason why it is crucial is that that suspicious node is having all the rights for accessing the information as any other network node .In this paper we will make use of a three stage model to identify the attacker node that is present in the network .Firstly, all the nodes checked for 3 properties throughput , energy ,delay to guess their behavior for abnormality. Secondly, neighbor nodes are made to check their properties that there are interacting normally. Thirdly , these are again checked with the use of evidences previously obtained that they are strong enough to prove the node as attacker one. If yes the node is removed from the network .The experiments gives appropriate results with the last stage.

Index Terms— Attacker , Dampster Shafer Theory ,3-level check algo , Energy, Nodes

I. INTRODUCTION

As a new type of network technology rising from the military field, WSNs can be widely applied to civil, commercial, medical field and other critical ones. Covering which the security problems are more important and noticeable. In WSNs, the attacks are complicated and various, the threats faced by WSNs are not only from external attackers, but also from internal nodes which are a part of the communication due to the rights allotted to them for network use. In such a systems it becomes difficult to mark which one is attacker or suspicious .If a right one is marked as attacker it may cause remarkable harm to the network information as that node become aware of checking, & behave intelligently in inspection of network. Another reason is that comparing with the external attacks, the internal attacks are more difficult to defense because that the key mechanisms are ineffective for internal malicious nodes, thus the internal attacks can make worse threats to the network. So it needs to be solved urgently for the legitimate nodes to detect and further eliminate the malicious nodes.

WSN is a network with functionality as:

Sensing + Processing + communication

Sensing-

It is storing of information i.e. collected data about any change in the defined property likewise temperature, pressure , moisture etc. It is the recording of physical data about any parameter .After that, it transmits it to the controller for further processing.

***Processing*-**

It takes the data from sensors & processes it and supervises the other components of the node .The processor may be micro controller, desktop microprocessor.

***Communication*-**

Sensor nodes often make use of ISM band, which includes free radio, spectrum allocation and global availability. The possible choices of wireless transmission media are radio frequency (RF), optical communication (laser) and infrared. Lasers communication requires less energy, but need line-of-sight for successful communication and is sensitive to atmospheric conditions. Infrared, like lasers, needs no antenna but it is limited in its capacity of broadcasting.

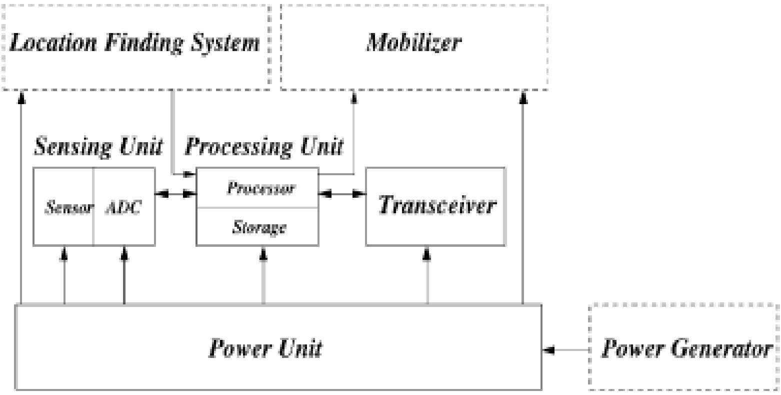


Figure 1: Components of WSN sensor node

Related Work-

Presently, the manners of identifying the malicious nodes of WSNs as follows:

A statistics-based malicious node detection scheme is

proposed by Ana Paula. A series of regulations are predefined to define the normal behaviors of nodes and further judge the anomaly or any deviation in behaviors of nodes, there is no interaction among nodes, so the rate of false alarming is quite high.

A rule-based malicious node detection scheme in Ad Hoc is proposed by

Chin-Yang].This scheme uses the monitoring points distributing in the network to monitor nodes whether operate in accordance with the routing norms in the process of AODV route query phase, then a finite state machine formed by the norms is used to identify nodes as normal state, suspected state, and intrusion state.

A Markov Chain based anomaly detection algorithm proposed by Bo Sun. This algorithm only aims at identifying the malicious nodes which launch route spoofing attacks, and needs to preserve a large amount of status information about changing of routing table. So it is not suitable for the resource-constrained sensor networks.

ACK based anomaly detection algorithm is proposed by

D. Tian and N. D. Georganas. In this algorithm, a next-hop

ACK feedback technology is used to identify the unreliable

communication links.

A checkpoint-based multi-hop acknowledgement scheme

for detecting selective forwarding attacks is proposed by Bo

Yu . In this scheme, part of intermediate nodes along a forwarding path can be randomly selected as checkpoint nodes which are responsible for generating acknowledgement for each packet received. On receiving an incident packet, a checkpoint will create an ACK for this incident packet and upstream transmit the ACK along the routing path. If an intermediate node does not receive a sufficient number of ACK packets, an alarm packet which designates its downstream neighbor node as the suspicious node will be created and transmitted to the source node by such an intermediate node.

Proposed Work-

In this work we give a algorithm for detecting the suspicious node with a 3 degree confirmation model. In this algorithm WSN is created with predefined no. of sensor nodes which are checked for communication under specified parameters i.e. energy , throughput , Delay time .

In our work , these parameters play a important role for the evaluation of a node to be suspicious or normal .Its behavior is checked either it is normal or abnormal .That means more energy , more delay , and high throughput or u pretended throughput .

Secondly , It is checked by a set of neighbor nodes .In other words a set of monitoring nodes are assigned for the purpose of rechecking the behavior of the above saved suspicious nodes so that non confusion or mistake could be there in decision .

Thirdly, Saving all the evidences of above checking, Evidence –belief theory is used for checking the plausibility & belief of these evidences .This theory implemented to find out the correctness of the doubt on the said node.

Evidence theory -a degree of belief also called mass is represented as a belief function. Probability values are assigned to *sets* of possibilities rather than single events: their appeal rests on the fact they naturally encode evidence in favor of propositions.

Shafer's framework allows for belief about such propositions to be represented as intervals, bounded by two values, *belief* (or *support*) and *plausibility*:

belief ≤ *plausibility*.

Here, subjective probabilities (*masses*) are assigned to all subsets of the frame; usually, only a restricted number of sets will have non-zero mass (*focal elements*). *Belief* in a hypothesis is constituted by the sum of the masses of all sets enclosed by it. It is the amount of belief that directly supports a given hypothesis or a more specific one, forming a lower bound. *Belief* (usually denoted *Bel*) measures the strength of the evidence in favor of a proposition *p*. It ranges from 0 (indicating no evidence) to 1 (denoting certainty). *Plausibility* is 1 minus the sum of the masses of all sets whose intersection with the hypothesis is empty. Or, it can be obtained as the sum of the masses of all sets whose intersection with the hypothesis is not empty. It is an upper bound on the possibility that the hypothesis could be true, *i.e.* it “could possibly be the true state of the system” up to that value, because there is only so much evidence that contradicts that hypothesis.

The algorithm works as follows:

This algorithm works in 3 stages Initial Check, Monitor Check, Belief Check

Initial Check:

In this a network is designed of WSN nodes including sensor nodes , One Base Station , some of the suspicious nodes.

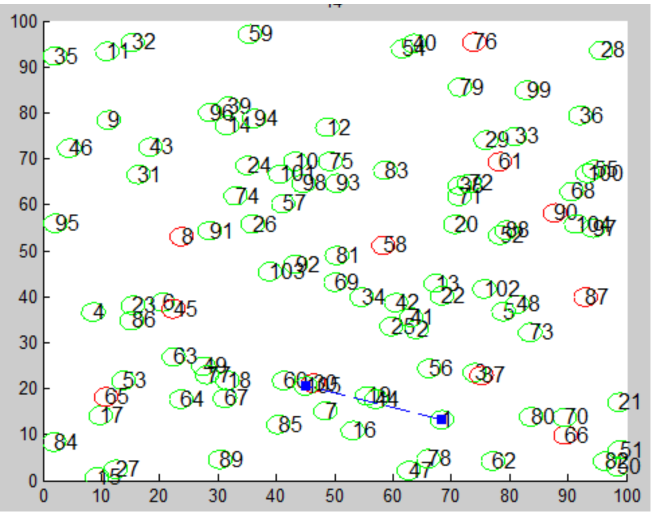


Figure 2: Designing a Sensor network with BS and attacker node

Initially all the parameters of network is set to the initial values i.e. Energy, delay , receiving ,transmitting signals etc. These parameters are updated timely according to the communication between the nodes and processing of information

Monitor Check:

In this check all the suspicious nodes are made under checking with the assignment of some of observer nodes / monitor nodes that keeps a supervision on the communication with these nodes. If found abnormally behaving ,saved for next stage check .

These checking is done by making 100s of looping or iterations so that no mistake could be left in the decision in checking the attacker one .Using of iteration has its purpose that in single transmission node may behave abnormal due any positive reason & in other iteration it could behave normal. No risk could be taken in this guessing as that attacker node has authorization rights & that node could harm in a second .

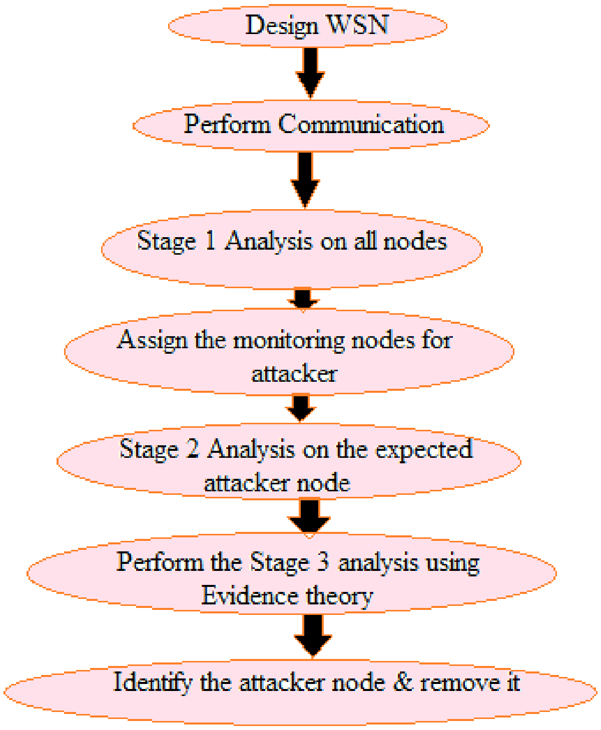

Design WSN
Perform Communication
Stage 1 Analysis on all nodes
Assign the monitoring nodes for attacker
Stage 2 Analysis on the expected attacker node
Perform the Stage 3 analysis using Evidence theory
Identify the attacker node & remove it

Figure 3: Working of complete algorithm

Belief Check:

The last check is Belief Check or the Evidence theory check .In this , we check the beliefs and plausibly on the certainity or probability of the attacker node present in the network . Bounded by two values, *belief* (or *support*) and *plausibility*:

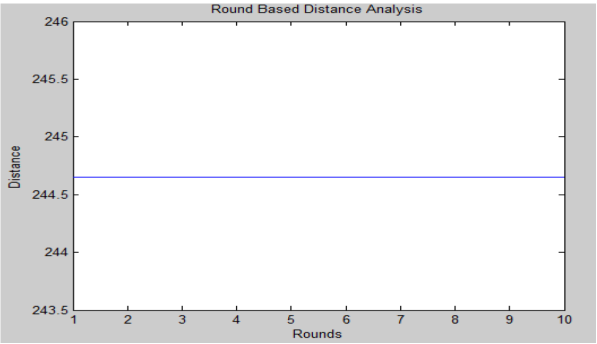


Figure 4: showing Distance covered in communication

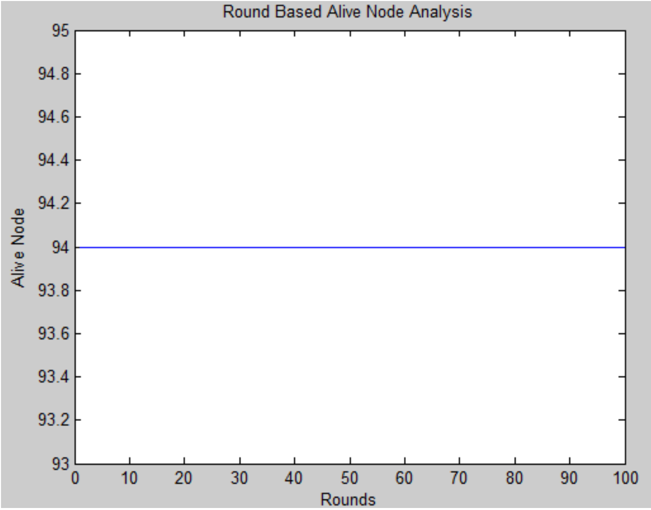
belief ≤ plausibility

Evidence Theory Checks the evidences arrived from the previous stage results and compare the results with its own values .

In this check we also use the iterations for the purpose of being sure about our decision .Here two types of nodes are made in this theory –Alive nodes , Dead nodes. Alive nodes which covers the belief , Dead nodes which cancels the beliefs or does not stand with belief.

Our focus is on the alive nodes as these nodes could be attacker nodes .Hence checked with 100s of iterations giving accurate results when implemented on Matlab environment .

. **Figure 5: showing the Dead nodes list**



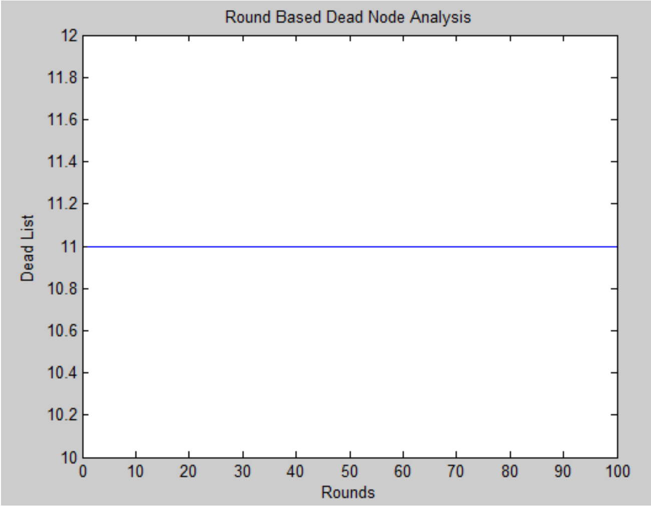


Figure 6: Showing Alive nodes list

After no. of iterations completed, this theory gives the result about the attacker nodes using parameters of energy, delays, throughput.

Conclusion:

WSN security is such a critical issue as these network gives very crucial information & are not supposed to be wrong in information. We make a algorithm for a 3 level check on the identification of the intruder node detection in case of sensor network .Previously no. of protocols are created for these networks for the security but our work is not so much complex as compared to those protocols .We give a algorithm simple to implement on network. With use of evidence theory , there is scope of use of any other theory in this work .

Future Scope:

With the vast area of applications i.e. military ,medical , air services etc. these networks require more secured data service. Hence in our work other theories could be added for more safer & quick results .Another concept that could be added is the manipulation of network or acquisition of change dynamically keeping the working of security algorithm same .This flexibility is needed to be there for network to accommodate more changes with changing environment .

References:

[1] Muhammad R Ahmed," A Novel Two-Stage Multi-Crieteria Evaluation for Internal Attack in WSN", 2013 13th International Symposium on Communications and Information Technologies (ISCIT) 978-1-4673-5580-3/13 © 2013 IEEE

[2] Guisheng Yin," A Novel Reputation Model for Malicious Node Detection in Wireless Sensor Network", 978-1-4244-2108-4/08 © 2008 IEEE

[3] Jerzy Konorski," Data-Centric Dempster-Shafer Theory-Based Selfishness Thwarting via Trust Evaluation in MANETs and WSNs", 978-1-4244-6273-5/09 ©2009 IEEE

[4] Wassim Znaidi," Hierarchical Node Replication Attacks Detection in Wireless Sensors Networks", 978-1-4244-5213-4/09 ©2009 IEEE

[5] Ochirkhand Erdene-Ochir," Resiliency of Wireless Sensor Networks: Definitions and Analyses", 2010 17th International Conference on Telecommunications 978-1-4244-5247-7/09 ©2009 IEEE

[6] Wu Yang," Research on Reputation Evaluation Model for WSN Nodes Based on Vertical and Horizontal Analysis", 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing 978-0-7695-4011-5/10 © 2010 IEEE

[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