International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:11, No:1, 2017

Detecting and Secluding Route Modifiers by Neural Network Approach in Wireless Sensor Networks

C. N. Vanitha, M. Usha

***Abstract*—**In a real world scenario, the viability of the sensor networks has been proved by standardizing the technologies. Wireless sensor networks are vulnerable to both electronic and physical security breaches because of their deployment in remote, distributed, and inaccessible locations. The compromised sensor nodes send malicious data to the base station, and thus, the total network effectiveness will possibly be compromised. To detect and seclude the Route modifiers, a neural network based Pattern Learning predictor (PLP) is presented. This algorithm senses data at any node on present and previous patterns obtained from the en-route nodes. The eminence of any node is upgraded by their predicted and reported patterns. This paper propounds a solution not only to detect the route modifiers, but also to seclude the malevolent nodes from the network. The simulation result proves the effective performance of the network by the presented methodology in terms of energy level, routing and various network conditions.

***Keywords*—**Neural networks, pattern learning, security, wireless sensor networks.

I. Introduction

SENSORS in wireless networks are deployed to sense the entire environment collaboratively to acquire potential information. The acquired data from the sensors are aggregated to provide final results. The sensors are deployed in various locations over a wide range, especially in many critical environments, such as military zones, seismic area, disaster locations, ecological sites, etc. The sensors play a vital role in harsh and hazardous environments. In such as the deployment phase, if any malfunction occurs, the complete environment tends to be damaged.

Wireless Sensor Networks always faces power consumption problem and security issues. In regard to security issues, the malicious node, which deviates from the route, will lead to an energy drain in the sensor nodes. Thus, the malfunctioning mote will impair the network in terms of both energy and security. Even though, many cryptographic algorithms emerge to identify a malicious node, they reduce the battery power in discovering whether the mote is a fault node [1]. To solve this issue, if the node is predicted as the malicious node earlier, by previous recorded patterns of the node, the data will be secured and energy also preserved.

Many vulnerable attacks such as hello flood, eaves dropping, wormhole, Sybil, and spoofing cannot be solved by cryptography alone. In wireless sensor networks, the biggest threat is node-capturing attack [2]. By this attack the sensor node is fully captured and the adversary takes complete control over the node. This type of attack is not fully dependent on internal security loop holes, like protocols, operating system, broadcasting, and connectivity, etc. It mainly depends on the deployment of the sensors in geographic positions.

Due to the enormous deployment of sensors in an unattended environment it is not possible to protect the entire network from the adversary. Added to this, sensors are easily attackable, and that leads to the damage and need for replacement of sensors [3]. Usually, sensors are deployed with the same operating system. To find an error, reverse engineering techniques should be used. This process helps the cyber punk to capture the sensor and manipulate the entire network.

The presented algorithm relies on the fact, even if the malicious node transmits authenticated data by using the previously stored cryptographic values to the base station. Thus, the PLP methodology:

- Identifies the cyber punks, and
- Secludes the malicious node from the network, by using Learned Patterns from the en-route nodes using neural networks.

II. Extract of Literature

Annadurai et al. [4] proposed a trust value methodology in cluster based MANET. In this method, they always trust on the cluster head; if the cluster head is an intruder or it fails, the entire network will be impaired. Trusting a single node in a network is not a good decision to maintain a network.

Patel et al. [5] surveyed the detection of the malevolent nodes by the various behaviors of the nodes. The behavior is identified using reinforcement, supervised and unsupervised techniques. They used various techniques such as, Q-learning, decision tree and vector machine. But in this survey they have not focused on speculating the malicious node rather than detecting them.

Heena et al. [6] developed a consensus-aware socio psychological trust model. They *trust* on the computation of the ability and integrity of the nodes in the network. However, we cannot give assurance of integrity all the time, because any node can be malevolent at any time.

Vanitha et al. [7] proposed a data filtration scheme using a rekeying mechanism. This method may drain the sensor's energy in checking the node and filtering the data. If it is previously predicted, the energy will be saved. Rather, the power of the sensor is reduced in rekeying the cipher keys.

C.N. Vanitha, Assistant Professor, Department of Computer Technology, Kongu Engineering College, Perundurari, 638 052, India (corresponding author; phone: +91 9003962637; e-mail: vanithacn.ctug@ kongu.ac.in).

M. Usha, Principal, Sona College of Technology, Salem – 638 005 (e-mail: usha@sonatech.ac.in).

Usha et al. [8] elaborated the pruning algorithm which identifies the malicious node and prunes that node from the route. The algorithm uses Poisson probability to measure the pruned nodes to update the reputation of the network effectiveness. After identifying the malicious node, pruning is done. The energy is minimized by this process. If we predict the malevolent node previously, it is easy to boycott the route to save energy.

III. System Model

A. Seculating Malevolent Node Using the Pattern Learning Process

Sensor nodes are deployed either by physical installation or by aerial scattering and it is static. Mostly, all the sensors are equal in battery power, communication and capability in computation. The authentication procedure and storage capabilities are also the same for the sensors which are deployed in the same environment.

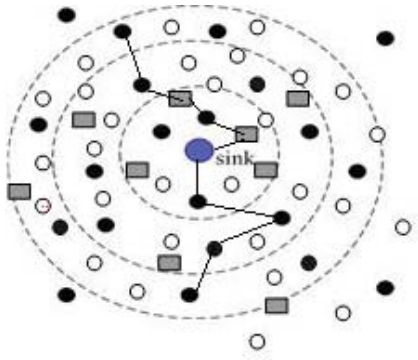

Fig. 1 Deployment of Sensors

Fig. 1 shows the deployment of sensors in an experimental environment and a sample route is established for transmission. Various active sensors are shown in dark color and sleep sensors are denoted in white color. The active sensors pass by the nearest neighbor active nodes and the router in the transmission path. All the sensed data is routed to the sink and the aggregated data is passed to the base station.

The sensor stores all the symmetric cryptographic cipher keys in the space allocated in the storage [9]. In a wireless sensor network deployment area, it is assumed that the location of the sensor node physically is i, in the distributed sensor region (a_i, b_i) which has n number of nodes. The node tree is formed hierarchically assuming the base station as the root node. The nodes in other levels aggregates the information obtained by its siblings and sends it to its parent. In every periodic time interval p, the sensed data value is calculated by the function (a_i, b_i, p) = g(a,b) +h(p) +A(μ,σ) , where time range is mapped to h, μ represents mean, σ standard deviation.

The offset generated randomly by sensing is used to identify malevolent nodes. The compromised nodes are mostly at leaf level, except the root i.e., control node. The sensors should report their reputation in the periodic interval p, and the threshold for the detection is assigned to a fraction p=0.04.

B. Pattern Learning Process

The reputation of the sensor networks is updated periodically by their previous and present data. The node redundancy is applied here to cover the entire sensor environment. The adjacent nodes are employed to prove the rightness of the information provided by the sensors.

The substitute sensors play a vital role in case of a malfunctioning situation. These sensors are used to choose the original data supplied or sensed by the majority of the sensors.

C. The Mathematical Approach

Mathematical model is highly helpful for calculating the effectiveness of the network [10]. Let 'L' be the active time of the entire network. Assume 'μ and σ' as the rate of activeness and rate of malevolent nodes, respectively, considering $0 \leq \sigma \leq \mu$. The benevolent node's probability is 'p_1'. Same as 'p_2' is the probability of a malevolent node. Random Variable x such that, for benevolent nodes x=0, x=1, if the node's behavior is abnormal during forming a Route. x=2, the nodes past values is abnormal in Reply. The residual energy of a node is 'r'. The time t1 is the failure time.

First, the Probability mass function of the Random Variable 'x' is as:

$$P_x(0)=\mu(1- p_1)/ \mu+ \sigma \quad (1)$$

$$P_x(1)=\mu(p_1)/ \mu+ \sigma \quad (2)$$

$$P_x(2)=\mu(1- p_2)/ \mu+ \sigma \quad (3)$$

Here the energy of node is given by (L1+L2) + r because the distributed parameter is μ +σ. The survival rate of a normal node is given by (4):

$$L_{y\acute{x}}(s\acute{x}=0)= \mu+ \sigma / s+\mu+ \sigma = L_{y\acute{x}}/(s/x=3) \quad (4)$$

The above survival rate is calculated by conditional Laplace transform of X.

The active rate of a malevolent node, either in route request or on route reply node, is given by (5):

$$L_{y\acute{x}}(s\acute{x}=1)= \mu+ \sigma / s+\mu+ \sigma[\mu p_1+ \mu p_2 /\mu+ \sigma] \quad (5)$$

The total transform is:

$$L_{y\acute{x}}(s)= \mu+ \sigma / s+\mu+ \sigma[\mu p_1+ \mu p_2 /\mu+ \sigma^* s+ \mu+ \mu(1- p_1)+ \mu(1- p_2)] \quad (6)$$

Equation (6) provides the active rate of a network. Here $L_{x1}(s)= \mu+ \sigma / s+\mu+ \sigma[\mu p_1+ \mu p_2 /\mu+ \sigma]$

$$L_{x2}(s)= \mu+ \sigma / s+\mu+ \sigma[s\mu+ s+\mu /* (1-p)] \quad (7)$$

The total probability for the normal and malevolent node is:

$$p_s=p_1+p_2 \quad (8)$$

The active rate of a node is given by (9):

$$R_x(t)= (1-p_1)e^{-(\mu+\sigma)t} / p+\mu+ \sigma[\mu p_1+ \mu p_2 /\mu+ \sigma^* s+ \mu+ \mu(1- p_1)+ \mu(1- p_2)] \quad (9)$$

This mathematical approach is evenly spread into all the sensor nodes to improve the effective network.

IV. PLP Algorithm

Let
of the sensor be N.
Output value: v
Predicted value: v^
Reputation factor associated with every sensor node: r
Data value: a
Predicted values using past / present values: a^
Result: malevolent node detection
Initial value: Reputation factor r = 1
For i = 0; i> Total no sensors; i++ do
Compute Reputation factor of each sensor node N using past values
Assign the same reputation factor for all sensor nodes.
For each sensor the reputation factor = r_N
For each sensor N,
$a^N(t) = f(Z_N, nei (t-1)\ldots Z_N , nei(t-k), A_N)$
where,
$Z_N,nei(t-k) = (a_N,nei(t-k),\ldots a_N,nei\text{-}m(t – i))^T$
The data provided by all neighbor sensors (t-k), $a_N = (r_{N, nei},\ldots, r_{N\ neim})$
Where, m is the neighbor node of N, and t is the order.
Compare the present value $a_N(t)$ of the sensor with its predicted value $a^N(t)$ by computing the difference $d_N(t) = aN(t) – a^N(t)$
Update reputation of each sensor.
If Reputation factor r <= Reputation limit * en-route nodes value
then
Malevolent node according to PLP algorithm

The PLP algorithm and Fig. 2 explains clearly about the detecting and secluding in the malevolent node process. The PLP algorithm has taken the previous patterns of the sensors to identify the fault nodes. For this, the time interval t has been taken. In that periodic time interval, the nodes are sensed to predict the fault nodes. The previous pattern is compared with the present values using the mathematical model and the decision is taken whether to accept or not. If it is reputed, the node is accepted and the data transmission is happened otherwise the route is deviated and the alternate route is selected for transmission.

If any deviation found in the sensed values the node reputation is updated and that is pruned for further communication.

First in t = 1, θ = θ (X, t) where, θ is the sensed data at the time t, the pattern learning process predict the a^N and it is capable of keeping the past values safe. The decision is made of the statistical model and the reputation factor r_N is updated and transmitted to the next level of hierarchy.

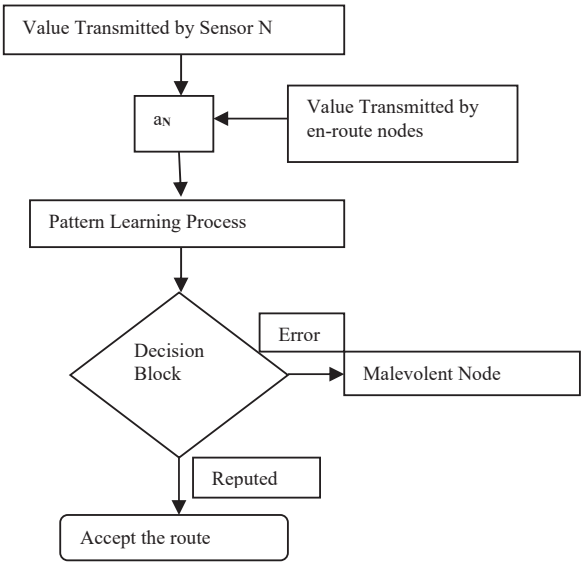

Fig. 2 Flowchart of PLP algorithm

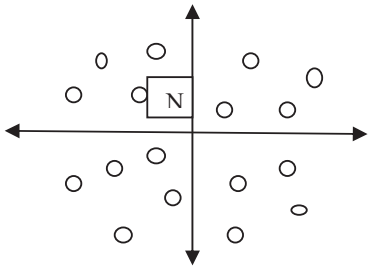

Fig. 3 Distribution of Sensors

In Fig. 3, the sensors are distributed because it is heterogeneous in nature. The current sensor is denoted as N, and the remaining en-route nodes are named as Ni where i= 1,2,3, …. The sensed data of the current sensor is θ_N. Apart from the security enhancement, the PLP algorithm also focuses the energy efficiency at every node.

$$dEi / dt = N_{in\text{-}x} – N_{out\text{-}y}$$

where E is the energy stored in Node x, initial energy of Node x and final energy of Node x is y after being predicted and transmitted.

V. Results and Discussion

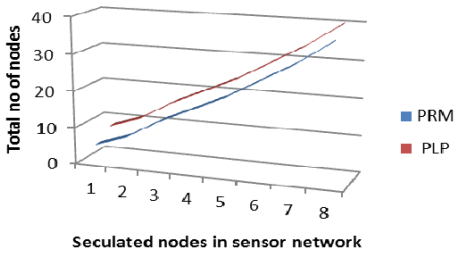

Fig. 4 Malevolent node detection with previous literature

Fig. 4 describes the speculated nodes among the total number of nodes deployed in sensor environment. Fig. 5 exposes the data transmission ratio among the malevolent nodes and the chart compares the performance of the transmission ratio with the previous literature.

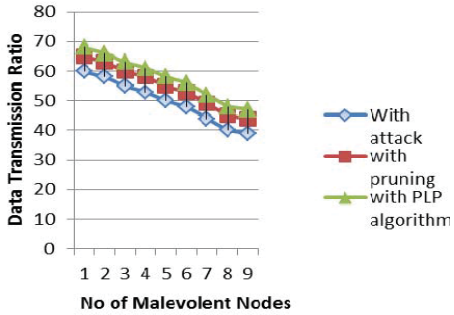

Fig. 5 Data Transmission ratio of detecting malevolent nodes

TABLE I
SIMULATION SETUP

Parameters	Value
Number of Nodes Simulation	200
Time	500 m/sec
Mac Layer	802.11
Transmission range	100m
Terrain Area	1500x1000 m^2
Traffic model	Constant bit rate
Mobility Model	Random way point
Deployment model	Random graph
Packet Size	512 bytes
Protocol	PSP
Packet Queuing	Drop tail
Type of Antenna	Omni Antenna

The Simulation setup to detect the malevolent node is shown in Table I. All the necessary parameters are discussed. The simulation proves its security enhancement in terms of the absolute identification of fault nodes.

VI. Conclusion

The experimental and simulation result shows that the sensors will not lose energy by malicious nodes. The pattern learning process works efficiently and successfully predict the malevolent nodes previously. This avoids the energy drain in the sensors. The prediction works 96% successfully for detecting and speculating intruders in the network. While comparing with the previous literature algorithms, the proposed PLP methodology works effectively in terms of energy and security and makes the network very efficient.

References

[1] Kyoungsoo Bok,1 Yunjeong Lee,2 Junho Park,3 and Jaesoo Yoo.” An Energy-Efficient Secure Scheme in Wireless Sensor Networks”, Hindawi, Journal of Sensors, Article ID 1321079, 11 pages, Volume 2016 (2016).

[2] C. Zhu, L. Shu, T. Hara, L. Wang, S. Nishio, and L. T. Yang, “A survey on communication and data management issues in mobile sensor networks”, Wireless Communications and Mobile Computing, vol. 14, no. 1, pp. 19–36, 2014.

[3] Tao Li; Pingyi Fan; Zhengchuan Chen; Khaled Ben Letaief, “Optimum Transmission Policies for Energy Harvesting Sensor Networks Powered by a Mobile Control Center”, IEEE Transactions on Wireless Communications, Volume: 15, Issue: 9 Pages: 6132 - 6145, 2016.

[4] P. Annadurai, S. Vijayalakshmi, “Identifying malicious node using trust value in cluster based MANET (IMTVCM), IEEE, International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 .

[5] Nirav J. Patel, Rutvij H. Jhaveri ,”Detecting packet dropping nodes using machine learning techniques in Mobile ad-hoc network: A survey”, IEEE International Conference on Signal Processing And Communication Engineering Systems (SPACES), 2015.

[6] Jheena Rathore, Venkataramana Badarla, Supratim shit “Consensus-Aware Sociopsychological Trust model for wireless sensor networks”, ACM Transactions on sensor networks(TOSN), Volume 12, Issue 3, August 2016.

[7] CN Vanitha, M Usha,” An Improved Version of Data filtration using Enhanced Routing Control Protocol in Wireless Sensor Networks”, International journal of Applied Engineering and Research, Volume 10, Issue No.46, pp.32036-32043, 2015.

[8] M. Usha, C. N. Vanitha, “Pruning Route Modifiers in Wireless Sensor Networks, Springer, Wireless Personal Communications, Volume 89, Issue 1, pp 27–43, July 2016.

[9] Kyung-Ah Shim,” A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks”, IEEE Communications Surveys & Tutorials, Volume: 18, Issue: 1, 2016.

[10] J. Sengathir, R. Manoharan, “Selfish Conscious Mathematical Model based on Reliable Conditional Survivability Co-efficient in MANET Routing”, Elsevier, 2013.

C. N. Vanitha received her M.E. degree in Computer Science and Engineering from Anna University, India in 2008. She obtained her M.Phil., M.Sc. and B.Sc. degree in Computer Science from Bharathiar University in 2004, 2002 and 1999, respectively. She is pursuing her doctoral degree at Anna University, India. She is a life member of ISTE. She is currently working as Assistant Professor in Department of Computer Technology with Kongu Engineering College, Perundurai.India. Wireless Sensor Networks, Networking and Security are her research interests.

M. Usha received her Ph.D. in Information and Communication Engineering and M.E. degree in Computer Science and Engineering from Anna University, India in 2008 and 1994 respectively. She obtained her B.E. degree in Electronics and Communication Engineering from Madras University in 1984. She is currently working as a Principal in Sona College of Technology, India. Her research interests include Quality of Service, Intelligence in Networking and Wireless Sensor Networks. She has more than 60 publications in journals and refereed conferences. She is the Chair of Computer Society of India, Salem chapter. She has authored a book titled ‘‘Computer System Architecture and Organization’’ published by Wiley India Publishers Ltd. She has been a reviewer in Elsevier Journal of Networks and Computer Applications since 2011. She has also been a reviewer for International Journal of Communication Networks and Distributed Systems (IJCNDS), Inderscience Publishers and for various international conferences. She is the recipient of ‘‘Best Woman Researcher— 2012 Award’’ conferred jointly by Computer Society of India, Salem chapter and Women Development Cell, Govt. College of Engineering, Salem.