2010 International Conference on Computer Application and System Modeling (ICCASM 2010)

Energy Prediction based Trust Manangement in Hierarchical Sensor Networks

Wen Shen[1] , Guangjie Han[1,2] , Mengli Cheng[1] , Chuan Zhu[1] , Gang Hu[1]
1Department of Information & Communication Systems, Hohai University, Changzhou, China
E-mail: hanguangjie@gmail.com, shen.wen1986@gmail.com
2Jiangsu Key Laboratory of Power Transmission & Distribution Equipment Technology, Changzhou, China

***Abstract*—Trust has been recently suggested as an effective security mechanism for wireless sensor networks (WSNs). In this paper, we propose an energy prediction based trust management that not only prevents the election of compromised or malicious nodes as cluster heads, but also introduce novel vice-head nodes to monitor the cluster heads' behaviors in case of their betrayal. Specifically, we employ energy prediction method to detect denial of service (DoS) attacks when nodes are electing trusted clusters. Also we present the scheme performance by simulations. The results show clear advantages of our trust approach in defending against denial of service (DoS) attacks in WSNs.**

Keywords-Trust; denial of service; Cluster; sensor networks; energy prediction

I. INTRODUCTION

Micro sensor nodes are normally vulnerable to various attacks. Security issues become very important for wireless sensor networks applications. Many WSNs are organized hierarchically to raise security. But they are still vulnerable to Denial of Service (DoS) attack. Typically, this attack usually launch Hello flood together with selective forwarding [1]. Thus, hierarchical sensor networks require specifically means to improve their security.

Trust has been recently suggested as an effective security mechanism to solve the problem [2]. The intent of establishing trust scheme is to ensure sensor nodes work faithfully by detecting and isolating malicious nodes.

In this paper, we introduce a novel energy prediction method to detect the Hello flood attack and also a trust management to defend against this mixed attack mentioned above. We propose a secure scheme EPTM (Energy Prediction based Trust Management) to establish trustworthy sensor networks. Without loose of generality, EPTM is simulated based on a classical routing protocol LEACH. Simulations show that EPTM can recognize attacks through energy prediction method then isolate malicious nodes within a round. Besides our approach decrease the probability of selecting malicious nodes as cluster heads to 20% even when 80% nodes are compromised. The following of this paper is organized as follows: section II presents some related work in the fields of trust mechanism in Hierarchical Sensor Networks. Section III develop an appropriate mechanism for trust management with our energy prediction design to secure the networks. Section IV shows the simulation result of our mechanism. Finally, section V concludes and outlines future work.

II. RELATED WORK

Trust management in hierarchical sensor networks is in its infancy state. To our knowledge, very few trust management is proposed specially for cluster-based sensor networks.

G.V.Crosby and N.Pissinou firstly introduced trust management to the cluster head (CH) election. After that, they proposed a frame work [3] that prevents the election of compromised or malicious nodes as cluster heads through trust based decision making. The authors simply evaluated all the nodes with the same Beta model. While consider the responsibility of cluster head node, it is reasonable to make a distinction with member nodes in establishing trust values.

Boukerch, etc. proposed a trust scheme ATRM [4]. The scheme is based on a clustered wireless sensor networks and calculates trust in a fully distributed manner. ATRM assumes that there is a single trusted authority which is responsible for generating and launching mobile agents that make it vulnerable against a single point failure. However this assumption may not be realistic in many applications.

Xu MD, etc. proposed TSRS [5], which puts forward a hierarchical trusted architecture for wireless sensor network, and establishes trusted congregations by three-tier framework. Nevertheless, the command nodes are supposed to construct with higher ability of computing and signal listening. While we think this assumption does not have a representative and made the network complicate. A simple and security efficient strategy based on homogeneous network is more desirable.

However, all these security researches in cluster-based sensor networks focused on how to select reliable and trustworthy cluster head to defend these DoS attacks, but they ignored the cluster head security after its election. During the life time of the sensor networks, packets delivery phase takes much more time than the cluster election phase. That means cluster nodes are more likely to be compromised after the election process even if they were trustworthy in the past. Therefore trust management of detecting and rejecting malicious attacks from betrayed malicious cluster heads is very critical. In this paper, we develop a new trust algorithm to solve this problem. A kind of energy prediction method is implemented to detect the Hello flood attack. Furthermore, we set a novel vice-cluster head to defend against the

978-1-4244-7237-6/$26.00 © 2010 IEEE

selective forwarding attack that betrayed cluster head would launch.

III. TRUST MANAGEMENT

A. EPTM Architecture

Our trust model is based on hybrid trust management scheme. Energy prediction method operates at the beginning of the cluster formatting phase. The detail of its function will be discussed in section *C*.

All nodes in the WSN will evaluate their trust value according to their past behaviors. Periodically, every node sends an evaluation packet to the base station to report whether itself worked legally, and we introduce a novel node named vice-head to ensure the trustworthiness of cluster heads. Vice-heads overhear the transmission between the base station and cluster heads. Once cluster heads launched denial of service attack, vice-head nodes will reduce their trust values and send alarm message to the base station.

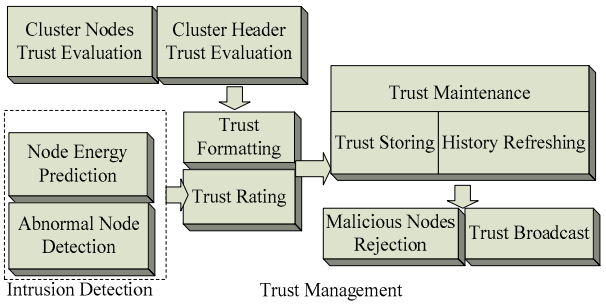

Figure 1. EPTM architecture

After the trust value collection, the base station will calculate the cumulative trust value of each node and quantize it. Depending upon that trust value, the base station will classify all nodes into one of the three possible domains: Trust domain, uncertain domain and untrust domain. After that, the base station will periodically multicast the current state of each node to cluster heads. The architecture of EPTM is shown in Fig.1

B. Intrusion Detection with Energy Prediction

Unlike usual trust managements which detect malicious attacks by accumulating trust value at sensor nodes, we adopt a novel energy prediction method to detect Hello flood attack.

Adversaries launch Hello flood attacks with extra energy cost which can be detected by nodes' energy prediction method. The node with abnormal energy dissipation is regarded as malicious or selfish. Our goal is to detect malicious nodes which launched Hello flood attack and prevent them from being selected as cluster heads. Working modes of nodes are represented by the states of a Markov chain [6] and the random variables represent the probability of staying in each state within a certain period of time. Assume the node is current in mode i ($X_0 = i$), the times that the node would stay in the mode s within t time-steps can be calculated by $\sum_{t=1}^{T} P_{is}^{(t)}$. Also, if assumed that E_s is the amount of energy dissipated by a node that remains in state s for one time-step, meanwhile the node is currently in state i , then the expected amount of energy spent in the next T times, E^T , is:

$$E^T = \sum_{s=1}^{M} (\sum_{t=1}^{T} P_{is}^{(t)}) * E_s \qquad (1)$$

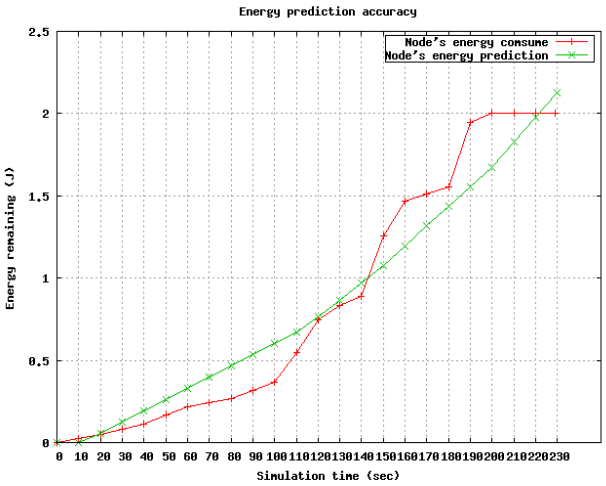

Figure 2. compared the energy prediction with actual dissipation

Using the value E^T , each member node in the cluster can calculate its energy dissipation rate ($\triangle E$) for the next T time-steps, then sends its available energy and $\triangle E$ to the cluster head. The cluster head can maintain an estimation of energy remaining in each node by decreasing the value $\triangle E$ periodically from the current energy in each node. Compared with the energy dissipate prediction, Cluster heads detect abnormal nodes send them to the base station where trust information is stored. The prediction result is shown in Fig.2

C. Trust evaluations at different levels

a) Individual Trust Evaluation at Cluster Level

Consider sensor nodes have the limited compute capacity, each member node's trust value is calculated simply by probabilistic model. We denote the set of all member nodes as $N = \{N_1, N_2, ..., N_n\}$ .The interaction trust value of N_j at Cluster node N_0 is defined as:

$$T(N_0, N_j) = \frac{S(j)}{S(j) + C(j)} \qquad (2)$$

$T(N_0, N_j)$ represents cluster node N_0 evaluates N_j by calculating the packet successful delivery rate, while $S(j)$ denotes as the successful times of forwarding data during a round, and $C(j)$ represents the failure times that

node j made in a round. Cluster head evaluates trust value of node $i(i \in 2,3,4,5,7)$ based upon whether they are able to accomplish a transaction with cluster head or not. Sensor nodes can be classified into five roles as shown in Fig.3.

Vice-head node is designed to ensure the trustworthiness of cluster head. Seeing that cluster head nodes make an important role in aggregating and transmitting packets, vice-head node is elected from trusted domain to monitor the header. The trust value of Cluster node at vice-head N_7 is defined as:

$$T(N_0, N_j) = \begin{cases} \left(\frac{S(j)+1}{S(j)+1+C(j)+1}\right) & success \\ \left(\frac{S(j)}{S(j)+C(j)+1}\right) & failed \end{cases} \quad (3)$$

The expression $\left(\frac{1}{C(j)}\right)$ approaches 0 rapidly with an increase of the failure times at node j. Hence function above will soon decrease the trust value of the cluster head once vice-head node found it malicious.

b) Trust Calculation at Base Station

Suppose there are *m* clusters in the network. Base station periodically multicasts request and receive packets from the cluster heads. On a request, cluster head forwards their trust evaluation of member nodes to BS. On the basis of these, BS will calculate with history trust value, and form a trust map of the whole network

$$T = \alpha_1 T_{present} + \alpha_2 T_{history} \quad (4)$$

Intrusion detection module operates at the beginning of the cluster formatting phase. If $E_i - \widetilde{E}_i > \varepsilon_1$ then this module believes Hello flood attack occurs. E_i represents the current energy remaining of node i, while $\widetilde{E}_i$ is the energy prediction value made in last round. ε_1 is the threshold. Once alarm message transmit to base station, the trust value of node i will decrease tremendously and the node will be regarded as malicious.

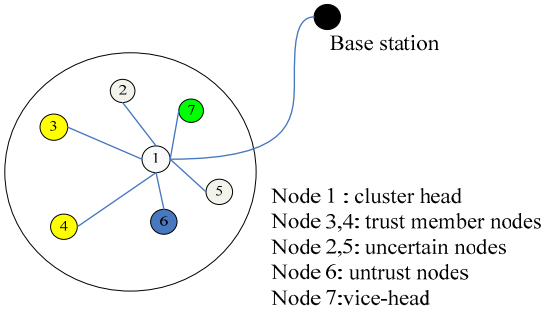

Figure 3. Nodes Characteristic Description

Base station is the center of sensor network and we suppose it doesn't have constraints of limited memory and power. Therefore, we can simply ignore the issue of security at the base station.

IV. SIMULATIONS

We use NS2 platform to simulate the performance of our model. 100 nodes are randomly deployed in 100 *100 m^2 area. A free space propagation model is assumed with a data rate set to 1Mb/s, each data message is 500 bytes long, and the packet header for each type of packet is 25 bytes long.

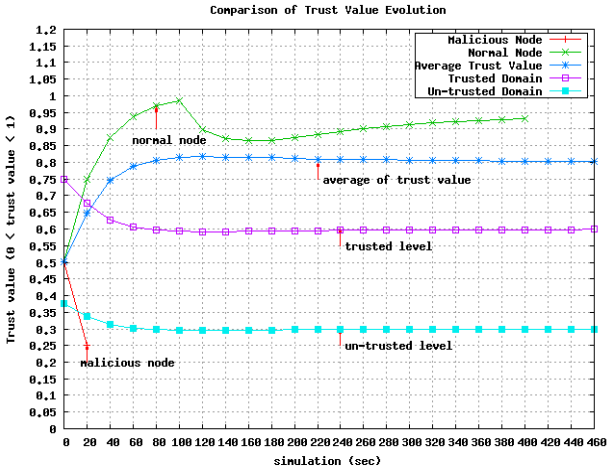

Figure 4. Comparison of Trust Value Evolution

In Fig.4, we assume that 20% sensor nodes are compromised. At the initialize phase, all the sensor nodes' trust value is set to be 0.5 with a trust level 0.75 and an un-trusted level 0.35. In the first 20s of the simulation, EPTM distinguish trusted and un-trusted nodes rapidly. After 60s, the average trust value of un-trusted nodes drop from 0.35 to 0.3. At the same time, trusted level falls from 0.75 to 0.6. That is because malicious nodes launch Hello flood attacks to win the cluster heads campaign and drop packets from the member nodes with a probability of 45%.Therefore, the trusted level and un-trusted level fall to adjust the changes of the trust values. While other normal nodes' trust value continually rise to nearly 1 as they honestly accomplished the transmission. After that, the average trust value stay at 0.8.

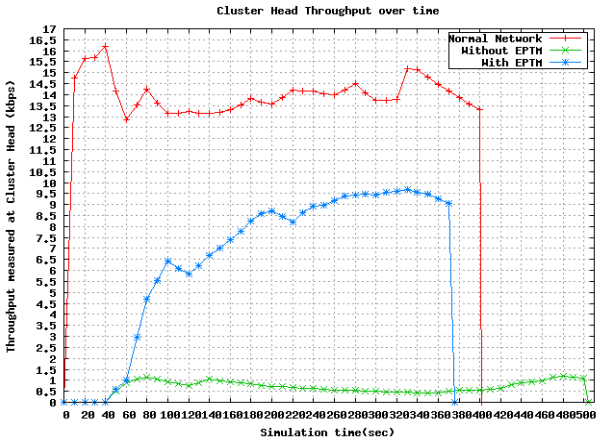

Figure 5. Throughputs at Cluster Head

Fig.5 shows EPTM solve selective forwarding attack by increasing the throughput at cluster heads. We assume that there are 20 malicious nodes with a 45% packet drop rate in the network. Without EPTM, this attack significantly decreases the throughput from 13.5kbps to nearly 1kbps. With EPTM, the throughput recovers back to 8.5kbps by detecting and isolating malicious nodes from the network, after that our mechanism chooses trusted nodes as cluster heads in order to transmit data packets to the base station.

V. CONCLUSIONS

In this paper, EPTM, a trust mechanism with energy characteristic is described. Energy prediction method is implemented to optimize cluster head election. We set vice-cluster head to prevent the damage that the betrayed cluster head would cause. It can be applied to defend against DoS attack by both detecting malicious nodes and preventing them to become cluster heads. The simulation results show clearly that providing an energy prediction based trust management in hierarchical networks can efficiently raise security. Future work involves rising malicious node detecting efficiency and extending our mechanism to defend against more inside attacks.

ACKNOWLEDGMENT

The work is supported by “the Excellent Master Research Funds for the Hohai University, No. XZX/09B011-02” and “the Fundamental Research Funds for the Central Universities, No.2010B22814, 2010B22914, 2010B24414 ”.

REFERENCES

[1] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE International Workshop on Sensor Network Protocols and Applications, pages 113-127, May 2003.

[2] Shaikh, R. A.; Jameel, H.; J. d’Auriol, B.; Lee, H.; Lee, S.; Song, Y.-J. Group-based Trust Management Scheme for Clustered Wireless Sensor Networks. In IEEE Trans. Parallel Dist. Sys.2009, 20, pp. 1698-1712.

[3] G. V. Crosby, N. Pissinou, Cluster-Based Reputation and Trust for Wireless Sensor Networks, Proceedings of 4th IEEE Consumer Communications and Networking Conference, pp. 604-608, January 2007.

[4] Boukerch, L. Xu, K. EL-Khatib, Trust-based security for wireless ad hoc and sensor networks, Computer Communications, 2007.

[5] Xu MD, Du RY, Zhang HG. A new hierarchical trusted model for wireless sensor networks. In: Proc. of Computational Intelligence and Security (CIS). Piscataway: IEEE Computer Society, 2006. 1541-1544.

[6] Sha Liu, Rahul Srivastava, Can Emre Koksal, Prasun Sinha, Pushback: A hidden Markov model based scheme for energy efficient data transmission in sensor networks, Ad Hoc Networks, Volume 7, Issue 5, July 2009, Pages 973-986