A Trust Evaluation Method Based on Energy Monitoring for Wireless Sensor Networks

Cunqun Fan, Shangguang Wang*, Qibo Sun, Hua Zou, Fangchun Yang
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications, Beijing, China
{fancunqun, sgwang*, qbsun, zouhua, fcyang}@bupt.edu.cn

I. INTRODUCTION

Wireless sensors have a wide range of applications, to realize the fusion of objects and existing internets. When the wireless sensor appears to increase diversification, corresponding security policy needs a better unified solution. Wireless sensors are not only confronted with external security threats, but also with the internal attacks that caused by the captured internal nodes. The traditional code security methods are mainly used for resisting the external attacks faced by nodes. There are also security authentication methods and trust valuation schemes used for network security, of which treating process is based on consuming the node's own energy. When in the field operation, the energy of wireless sensors cannot be supplied in time, which greatly impact on working life of the nodes.

Aiming at the problems that some researches of the node energy and its monitoring has been applied to wireless sensor network for solving excessive loss of energy. Goel and Imielinski [1] proposed an energy monitoring method of wireless sensors, which was used to solve energy efficiency monitoring by prediction module based on monitoring. The module's main function is to use the higher energy nodes to conform in the same task through monitoring the energy of sensors in wireless networks. In this way, this condition that the energy of lower nodes has been exhausted so as to impact on the service time of the whole wireless sensor network can be avoided. The authors [2] proposed a hierarchical approach for collecting residual energy information in the sensor network continuously in order to construct an energy map at the base station. Based on the energy information collected, a set of polygons which represent the contours of different energy levels are produced independently for each cluster.

In addition, researchers [3-5] also proposed some reference sensor trust evaluation methods. The authors [4] proposed the first deterministic distributed protocol for an accurate identification of faking sensors in a WSN. The scheme does not rely on a subset of trusted nodes that cooperate and are not allowed to misbehave. Thus, any subset of nodes is allowed to try faking its position. As in previous approaches, the protocol is based on distance evaluation techniques developed for WSN. Delaet et al. [5] proposed a trusted routing to locate and to preserve trusted routes in MANETs. Instead of using a hard security mechanism, they employ a new dynamic trust mechanism based on multiple constraints and collaborative filtering.

However, although the previous researches obtain some achievements, there still are some problems with resisting intrusion of adversaries and attacks of control. If the nodes were attacked and under controlled by the adversaries, the secret stored will be disclosed. Once the adversaries master the key of nodes, the security methods based on authentication cannot find the disclosing of the key in time, which can threaten the whole sensor networks. Hence, we choose accurate trust evaluation of sensors and optimizing the energy consumption of trust evaluation as the targets. In this abstract, we propose a trust evaluation method of sensors based on energy monitoring. The information about energy consumption is obtained by energy monitoring. By comparing the actual energy consumption with theory energy consumption and calculate them with the correlation coefficient method. And then we can judge the safety of the nodes status, according to the correlation. Simulation results show that the proposed method is proved to be high accuracy on the node trust evaluation, by which the unsafe nodes in the sensor network can be accurately distinguished.

II. THE TRUST EVALUATION METHOD

The state and behaviors of wireless sensor are basis to determine whether the node is credible. Controlled sensors will carry out some of the tasks that do not be set by the center, including sending data, sensor monitoring and so on. These behaviors of nodes are built on the foundation of the own energy consumption. Through monitoring and collecting the energy consumption of sensors and sending energy consumption information of sensors back to the monitoring center, the center will determine the behavior and state of the sensors periodically, as shown in Fig.1. And then the processing center will know whether the node is credible.

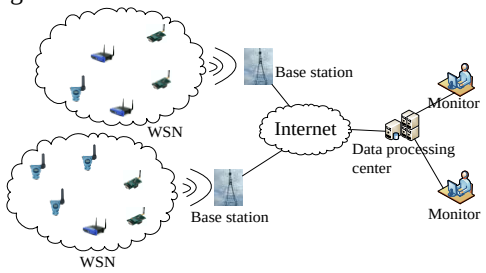

Fig. 1. Trust evaluation model based on energy monitoring

In order to confirm whether the node is in an abnormal state through energy consumption, we need to compare the actual

*Corresponding Author

and theoretical values of the node's current energy consumption reasonably, and then judge whether the node is in a non-secure state. The difference of the node energy consumption cannot be accurately expressed by using the simple linear difference comparison. Meanwhile the real-time synchronization comparison limits the energy of node consumption. So, we introduce the concept of correlation coefficients to compare.

The received data of each stage are the monitoring values of the energy consumption over a period of time *t'*. Thus, we can obtain the energy consumption power function $W_n(t)$ from a certain moment t_0 in time *t'*. The theoretical energy consumption power function $W_s(t)$ can be obtained in same time. So, we can obtain the correlation coefficient for $W_n(t)$ and $W_s(t)$ is given by

$$\begin{cases} \mathrm{Cov}(W_s, W_n) = E(W_s W_n) - E(W_s)E(W_n) \\ \rho_{sn} = \dfrac{\mathrm{Cov}(W_s, W_n)}{\sqrt{D(W_s)}\sqrt{D(W_n)}} \end{cases},$$

where ρ_{ns} is the correlation coefficient between W_n and W_s. In order to ensure the trust value may be of accurate distinction, we do a phased quantitative comparison on the basis of the correlation coefficient. We set two threshold values, and the correlation coefficient range is divided into three intervals. Trough re-analysis and calculation, we may determine whether the node is credible. Two threshold values are $\Delta\rho_1$ and $\Delta\rho_2$. Three intervals are $(0, 1-\Delta\rho_1-\Delta\rho_2]$, $(1-\Delta\rho_1-\Delta\rho_2, 1-\Delta\rho_1]$ and $(1-\Delta\rho_1, 1)$.

1) When ρ_{ns} belongs to the interval $(1-\Delta\rho_1, 1)$, the correlation coefficient between $W_n(t)$ and $W_s(t)$ is similar to a linear correlation. The actual energy consumption of the node is very close to the theoretical energy consumption. We can determine that the node is in a safe state, which means that the node is credible.
2) When ρ_{ns} belongs to the interval $(1-\Delta\rho_1-\Delta\rho_2, 1-\Delta\rho_1]$, the linear relationship between $W_n(t)$ and $W_s(t)$ is not very significant. We can determine that the node is temporarily in a safe state, which means that the node should be kept observation.
3) When ρ_{ns} belongs to the interval $(0, 1-\Delta\rho_1-\Delta\rho_2]$, the linear relationship between $W_n(t)$ and $W_s(t)$ is very weak. The actual energy consumption and theoretical energy consumption have great differences. We can determine that the node is in an unsafe state, which means that the node is suspect.

III. Preliminary Results

In this abstract, the trust evaluation mechanism can be used for most of the wireless sensors. There are no special requirements for application characteristics of sensors. In the simulation experiments, we have set 30-minute fixed tasks.

In the case of none attacks, the correlation coefficient between actual energy consumption and theoretical energy consumption is 0.993809. Based on fixed tasks, the experiments simulate the rival control attack and wormhole attack. In the case of control attack and wormhole attack, the correlation coefficient is 0.379975 and 0.794643, respectively, as shown in Fig.2.

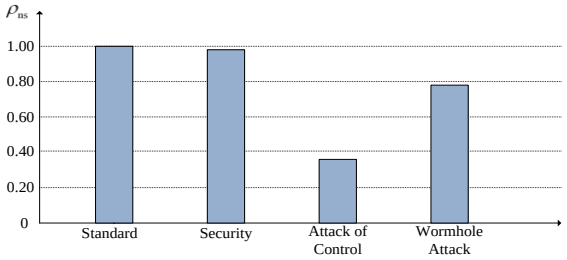

Fig. 2. Correlation coefficients

Under normal circumstances, if $\rho_{ns}>0.85$, we think that there is a strong linear relationship between them. In some applications, $\Delta\rho_1$ and $\Delta\rho_2$ can approximatively select the value 0.1 and 0.05, respectively. Simulation results show that the calculated correlation coefficients have a strong boundary between the safe nodes and unsafe nodes. The determination of the node security is provided with very high accuracy.

IV. Conclusion and Future Work

After acquiring the precise information about energy consumption, the trust degree of the nodes can be obtained through the calculation of correlation coefficient. It has low computational complexity, and the node trust value calculated considers the good discrimination. But because the energy information is delivered to the center by stages to calculate and evaluate, the security evaluation information cannot be absolutely real-time. Under the circumstances of amount of sensors deployed, large volumes of data back to the monitoring center will affect network efficiency to some extent. All of these problems need to be solved in the next stage.

Acknowledgements

The work presented in this study is supported by NSFC (61202435), NSFC (61272521), BMNSF (4132048), SRFDP (20110005130001), NCET (100263) and FIRGNNSFC (61121061).

References

[1] Samir G, Tomasz I. "Prediction-based Monitoring in Sensor Networks: Taking Lessons from MPEG," ACM SIGCOM Computer Communication Review, 2001: 82-98.

[2] Edward C, Song Han. "Energy Efficient Residual Energy Monitoring in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, 2009(5): 748–770.

[3] George T and John S. "On trust models and trust evaluation metrics for ad hoc networks," IEEE Journal on Selected Areas in Communications, 2006, 24(2):318-328.

[4] Peng SC, Jia WJ, et al. "Trusted Routing Based on Dynamic Trust Mechanism in Mobile Ad-Hoc Networks," IEICE Transactions on Information and Systems, 2010(3): 510-517.

[5] Delaet S, Mandal P, Rokicki M, et al. "Deterministic secure positioning in wireless sensor networks," Theoretical Computer Science, 2011, 412(35): 4471-4481.

*Corresponding Author