A Reliable and Energy-efficient Traffic Attack Detection Protocol for WSN

Bi Jiana
Department of Information Science and Technology
Bohai University
Jinzhou, China
bijiana@yahoo.com.cn

E Xu
Department of Information Science and Technology
Bohai University
Jinzhou, China
exu21@163.com

***Abstract*—How to accurately and rapidly detect traffic attack is an important security problem in wireless sensor networks. An energy-efficient ARMA-based traffic attack detection protocol is proposed in this paper. The detection protocol uses linear prediction to establish easy ARMA(2,1) model for sensor nodes. In the detection protocol, different nodes play different roles, and use different monitor schemes. Virtual cluster head and monitor nodes are elected. Monitor nodes monitor cluster head, and report to virtual cluster head. Virtual cluster head broadcasts abnormal cluster head to all member nodes, and initiates a new cluster head election. Member nodes are monitored by their cluster head. Simulation shows that, the detection protocol can real-time predict traffic attacks, and consume less energy. It not only protects sensor nodes against traffic attacks, but also prolongs the lifetime of network.**

Keywords-wireless sensor networks; security; traffic attack detection; ARMA

I. INTRODUCTION

Wireless sensor networks(WSN) are vulnerable to kinds of attacks [1-2]. The security of WSN is a difficult study subject [3-4]. Traffic attack is seriously harmful to WSN [5]. So traffic attack detection is paid more attention by researchers [6]. In cluster-based rooting protocols like LEACH, TEEN, APTEEN, PEGASIS and so on, cluster head receives and fuses data from cluster member nodes, and then transmits data to sink. So cluster head plays a more important role than its member nodes. While most cluster-based rooting protocols have no security protection for cluster head. When there are traffic attacks, cluster head will be main target for attackers. To obtain secure sensing data, it is necessary to use different schemes to monitor cluster head and members nodes. In WSN, every sensor node is possible to be captured, so a robust rooting protocol needs to bear captured nodes. In our traffic attack detection protocol, member nodes are monitored by their cluster head, and cluster head is monitored by special monitor nodes and virtual cluster head.

II. TRAFFIC MODEL AND PREDICTED TRAFFIC VALUE COMPUTING

Real-time network monitoring is a part of network management, and it can collect information of network states and actions. In general, detection of abnormal network traffic is realized by setting threshold value. Given the limited ability of senor nodes, we adopt easy linear prediction model — ARMA(2,1)(Autoregressive Moving Average).

A. Stabilize Data Sequence

We suppose that the size of the sliding window is n, and the sensing data traffic sequence is $T_0^{'}, T_1^{'}, \cdots, T_i^{'}, \cdots, T_n^{'}$. The data sequence is periodic, but it is not stable. In order to establish ARMA model, we take the logarithm of the data sequence and obtain the stable sequence $T_0, T_1, \cdots, T_i, \cdots, T_n$. Then we use the stable data sequence to establish ARMA model, and predict the first $n+1$ traffic value.

B. Establish Model

According to $T_0, T_1, \cdots, T_i, \cdots, T_n$, we establish ARMA model—$\phi(B)X_i = \theta(B)a_i$. B is backward shift operator. a_i is white noise, and it is independent and identically distributed random Gauss variable. Its mean value is zero, and its variance is σ_a^2.

$$\phi(B) = 1 - \phi_1 B - \phi_2 B^2 \quad (1)$$

$$\theta(B) = 1 - \theta_1 B \quad (2)$$

ϕ_1, ϕ_2, θ_1 are estimation parameters. We use least squares estimation method to solve $\hat{\phi}_1$, $\hat{\phi}_2$, $\hat{\theta}_1$, $\hat{\sigma}_a^2$. Then we judge the stability of data sequence on the estimated parameters. The stability conditions are as that:

$$\hat{\phi}_1 + \hat{\phi}_2 < 1 \quad (3)$$

$$\hat{\phi}_2 - \hat{\phi}_1 < 1 \quad (4)$$

$$\left|\hat{\phi}_2\right| < 1 \quad (5)$$

According to these stability conditions, ARMA model is established as that:

$$T_t = \hat{\phi}_1 T_{t-1} + \hat{\phi}_2 T_{t-2} + a_t - \hat{\theta}_1 a_{t-1} \quad (6)$$

Then we can predict by inverse function. The inverse function of ARMA is $N_1, N_2, \cdots, N_j$. So we can obtain that:

$$N_1 = \hat{\phi}_1 - \hat{\theta}_1 \quad (7)$$

$$N_2 = \hat{\phi}_2 - N_1 \hat{\theta}_1 \quad (8)$$

$$N_3 = N_j \hat{\theta}_1 \cdots (j > 3) \quad (9)$$

One step prediction model is as that:

Published by Atlantis Press, Paris, France.

$$\hat{T}_t(1) = \sum_{j=1}^{m} N_j T_{t-j} \quad (10)$$

In (10), m means that there are m observed values before T_t. The value of m can be changed according to prediction precision. One step prediction error e_t is as that:

$$e_t = T_t - \hat{T}_t = \sum_{j=0}^{m} N_j T_{t-j} \quad (11)$$

$$N_0 = -1 \quad (12)$$

III. VIRTUAL CLUSTER HEAD DETECTION

The operation cycle of cluster-based WSN is often a round. Each round includes cluster establishing stage and stable data transmitting stage. Our traffic attack detection protocol begins after cluster is established. In our detection protocol, stable data transmitting stage is divided into two stages. One is virtual cluster head and monitor nodes electing stage, and the other is united attack detection stage. At electing stage, member nodes elect m monitor nodes and a virtual cluster head according to their energy and a random function. The nodes which have much energy are easy to be elected. At united attack detection stage, when monitor nodes detect abnormal traffic behavior of cluster head, they transmit alarm information to virtual cluster head. Once the number of nodes which report alarm information to virtual cluster head exceeds threshold, virtual cluster head will broadcast the alarm information to all member nodes of the same cluster, and then initiate a new cluster head election. Monitor nodes and virtual cluster head are transparent to cluster head. Cluster head does not know they exist. Virtual cluster head receives alarm information from monitor nodes, but it does not receive sensing data. It can avoid member nodes from transmitting data to captured cluster head.

A. Virtual Cluster Head and Monitor Nodes Election

In this protocol, we use establishing cluster scheme of GDD [7] which is an energy-efficient and cluster-based rooting protocol we designed before. At establishing cluster stage, every node broadcasts its energy. So at the end of establishing cluster stage, every node knows its energy ranking in its cluster. When electing monitor nodes and virtual cluster head, the nodes which remain much energy have priority. While virtual cluster head is elected by monitor nodes among them by turns.

B. Detection Process

In our protocol, monitor nodes and virtual cluster head are elected among member nodes, and they are transparent to cluster head. Monitor nodes and virtual cluster head implement detection together. Monitor nodes monitor cluster head, and then report alarm information to virtual cluster head. Virtual cluster head broadcasts abnormal cluster head information to all member nodes. Monitor nodes only transmit alarm information of abnormal cluster head to virtual cluster head. Member nodes only receive alarm information of abnormal cluster head from virtual cluster head. When the number of monitor nodes which report abnormal cluster head exceeds threshold, virtual cluster head broadcasts information of abolishing old cluster head, and initiates a new cluster head election.

IV. DETECTING ABNORMAL MEMBER NODES

In cluster-based WSN, every member node transmits sensing data to its cluster head. So cluster head can detect malicious behavior of its member nodes. Once cluster head detects abnormal behavior of a member node, it can restrain the member node. In our detection protocol, member nodes are monitored by their cluster head. Every cluster head has an alarm table to record abnormal behavior of its member nodes. The alarm table includes two fields. One field records the ID of the suspected node, and the other records alarm times. When detecting abnormal traffic behavior of a member node, cluster head immediately updates its alarm table. Once the alarm times of a member node exceed threshold value, cluster head will broadcast ID of the member node, and delete it. Abnormal nodes can thus be restrained.

V. PROTOCOL PERFORMANCE ANALYSIS

GDD is an energy-efficient and cluster-based rooting protocol without security consideration we designed before. We take GDD as basic rooting protocol. At First, we compare GDD with GDD protected by our traffic attack detection protocol(IPD). And then we compare IPD with another traffic attack detection protocol(ESID) designed by Su [8].

A. Simulation Setting

We deploy sensor nodes in 140m×140m area, and let them sense temperature. All nodes are randomly deployed. There are 100 nodes in this area. Initial energy of node is 2J. Attackers use traffic attack, and they randomly attack these nodes to consume energy. Monitor error ratio of node is 5%.

B. Simulation without Attacks

1) Alive Nodes

Fig. 1 shows alive nodes of basic GDD protocol between GDD protected by IPD. The performances of them are similar before 300s. Difference appears after 300s. But there is no distinct difference between them. They remain similar decrement rate. This illustrates that rooting protocol protected by IPD has similar lifetime with basic rooting protocol when there are no attacks. So IPD is a lightweight detection protocol, and it is fit for WSN.

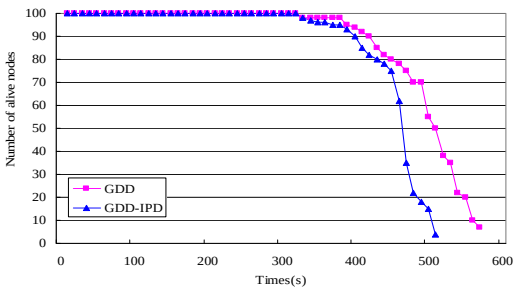

Figure 1. Number of total alive nodes

2)Energy Consumption

Fig. 2 shows energy consumption of nodes. The two curves of GDD and GDD protected by IPD are close to each other. It illustrates that IPD consumes less energy. It saves much energy of nodes. So IPD is an energy-efficient protocol.

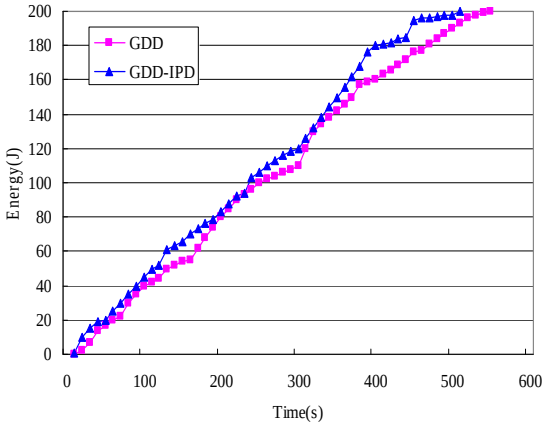

Figure 2. Energy consumption of nodes

C. Simulation under Attacks

1) Alive Nodes

Fig. 3 shows that, under traffic attacks, sensor nodes of basic GDD protocol die immediately. Network soon exhausts. GDD protected by IPD is almost not affected. At the same time, the lifetime of GDD protected by IPD is longer than GDD protected by ESID.

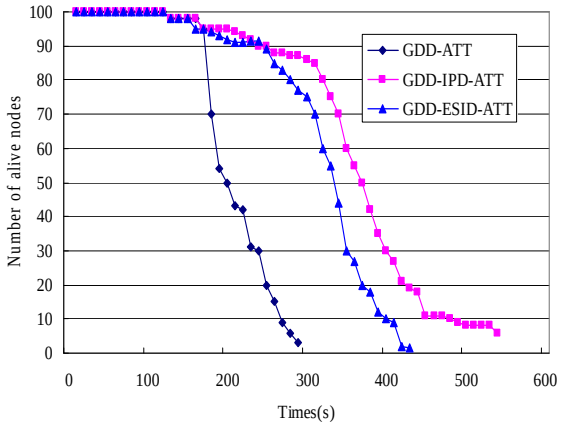

Figure 3. Number of total alive nodes

2)Energy Consumption

Fig. 4 shows that, there curves are similar before 100s. IPD has advantage after 100s. Under traffic attacks, energy of nodes in basic GDD is consumed very seriously. Nodes nearly consume all energy at 300s. In GDD protected by ESID and IPD, network can avoid malicious nodes, because there are attack reflection schemes. In GDD protected by ESID, energy of nodes remains until 400s. In GDD protected by IPD, energy of nodes remains until 500s. So IPD protocol is excellent in energy consumption.

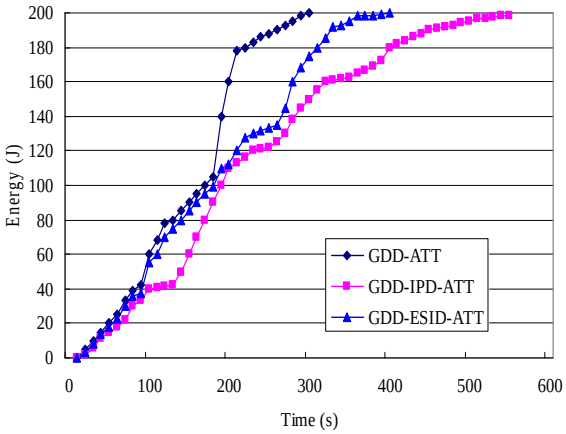

Figure 4. Node energy consumption

D. Detection Ratio of Captured Nodes

Detection ratio of captured nodes reflects correctness of detection protocol. A good detection protocol can avoid captured nodes. Detection ratio of captured nodes is affected by ratio of captured nodes and density of nodes.

1) Ratio of captured nodes

Fig. 5 shows detection ratio of captured nodes of ESID and IPD under different ratios of captured nodes. IPD has a higher detection ratio than ESID. But with more captured nodes, detection ratio of two detection protocols all descend. This can be explained that, the more captured node, the more incorrect information received by nodes. Incorrect judgments increase, and detection ratio descends.

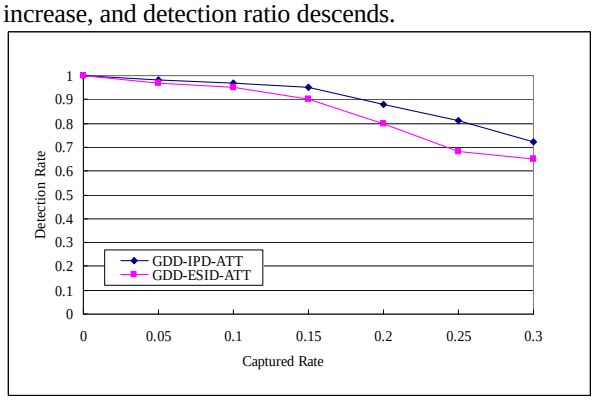

Figure5. Ratio of captured sensor nodes

2) Density of nodes

Fig. 6 shows detection ratio of IPD and ESID under different densities of nodes, when ratio of captured nodes is 20%. We deploy 5 groups of nodes in 140m×140m area. The number of nodes is from 20 to 100. As is shown that, with density of nodes increasing, detection ratio increases. With more neighbors, nodes can obtain more information to make correct judgments.

Published by Atlantis Press, Paris, France.

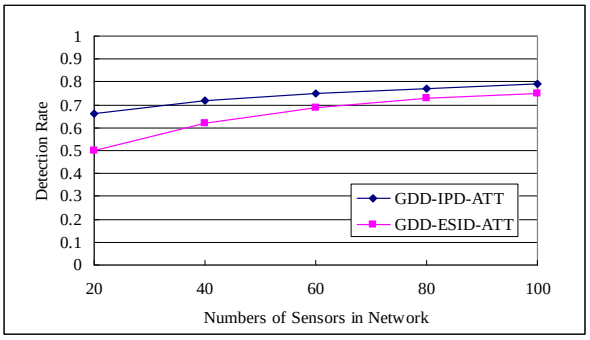

Figure 6. Density of sensor nodes

VI. CONCLUSION

In this paper, we propose an easy and energy-efficient protocol to protect sensor nodes from traffic attack. We use ARMA(2,1) and linear prediction technique to establish traffic prediction model. At the same time, we use different monitoring schemes for different kinds of nodes. Virtual cluster head and monitor nodes are elected among member nodes. The election of virtual cluster head and monitor nodes is transparent to cluster head. Monitor nodes monitor cluster head, and report alarm information to virtual cluster head. Virtual cluster head receives and records alarm information of abnormal cluster head. Once malicious cluster head is confirmed, virtual cluster head will broadcast the abnormal cluster head information to all member nodes, and initiate a new cluster head election. Member nodes are monitored by their cluster head. Simulation shows that, our traffic detection protocol is a lightweight one. It can effectively protect sensor nodes from traffic attacks, and prolong lifetime of network.

ACKNOWLEDGMENT

The paper is supported by the National Natural Science Foundation of China(No. 61203002), the Project of Liaoning Province Office of Education(No. L2012396, No. L2012397, No. L2012400), and Postdoctoral Science Foundation of China(No. 2012M520158).

REFERENCES

[1] I. Onat and A. Miri, “An Intrusion Detection System for Wireless Sensor Networks,” Proc. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, IEEE Press, Dec. 2005, pp. 253-259.

[2] A. Da-Silva, M. Martins, and B. Rocha, “Decentralized Intrusion Detection in Wireless Sensor Networks,” Proc. the 1st ACM International Workshop on QoS and Security for Wireless and Mobile Networks, Jan. 2005, pp. 16-23.

[3] S. Rajasegarar, “Distributed Anomaly Detection in Wireless Sensor Netwoks,” Proc. the 10th IEEE Singapore International Conference of Communication System, IEEE Press, Nov. 2006, pp. 1-5.

[4] A. Agah, S. Das, and K. Basu K, “Intrusion Detection in Sensor Networks: A Non-cooperative Game Approach,” Proc. IEEE International Conference on Communications, IEEE Press, Fri. 2005, pp. 3218-3222.

[5] R. Roman, and J. Zhou, “Applying Intrusion Detection Systems to Wireless Sensor Networks”, Consumer Communications and Networking Conference, vol. 16, Jan. 2006, pp. 640-644.

[6] J. Deng, R. Han. “Defending against Path-based DoS Attacks in Wireless Sensor Networks,” Proc. the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Dec. 2005, pp. 89-96.

[7] Bi Jiana, Ji Zhenzhou, and Cao Zhiyan, “Grid-based directed diffusion for wireless sensor networks”, High Technology Letters, vol. 14, Nov. 2008, pp. 342-347.

[8] C. Su, K. Chang, and Y. Kuo, “The New Intrusion Prevention and Detection Approaches for Clustering-based Sensor Networks,” Proc. IEEE Wireless Communications and Networking Conference, IEEE Press, Mar. 2005, pp. 1927-1932.