Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13)

A Secure and Energy-efficient Rooting 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*—In directed diffusion rooting protocol, interest and exploratory data are disseminated by flooding, which will bring broadcast storm resulting in substantial energy consumption of wireless sensor networks. Grid-based directed diffusion rooting protocol can improve energy efficiency where geographic grids are constructed by self-organization of nodes using location information. Flooding of interest and exploratory data is limited in grid head nodes. But grid-based directed diffusion rooting protocol considers less about security. To adapt to environments with high security requirements, traffic attack detection and secure data aggregation schemes are added to grid-based directed diffusion rooting protocol. Simulation shows that the proposed schemes can real-time predict traffic attacks and improve accuracy of data aggregation results when networks are under attacks. At the same time, the protocol consumes less energy and extends lifetime of networks.**

Keywords- wireless sensor networks; security; traffic attack detection; data aggregation

I. INTRODUCTION

Due to limited battery capacity, minimizing energy consumption is a key requirement in the design of wireless sensor networks(WSN). Directed diffusion(DD) [1] is a robust, scaled rooting protocol for WSN. Although DD provides a reliable and robust rooting scheme, flooding of interest and exploratory data is its shortcoming. This results in increased channel contention and waste of bandwidth that will take further toll on the scarce energy resource of sensor nodes.

The problem is resolved by grid-based directed diffusion(GDD) [2]. In GDD, network area is first divided into fixed grids. In each grid, one grid head is elected to forward interest and sensing data. Due to rest nodes only receiving interest from grid head and sending data to grid head, broadcast overheads are reduced. As WSN is usually deployed in open areas, sensor nodes are susceptible to a variety of attacks. A few authentication schemes have been proposed to prevent outside attackers, and they often use message authentication codes and key distribution schemes [3]. But they can not avoid injection of the forged data from malicious compromised insider nodes which have already been authenticated as legal ones in the networks. Some insider attack detection schemes based on statistics, hidden Markov model, data mining [4], game theory, and trust management [5] have been proposed. While they need more storage and computing resources of sensor nodes, and extra communications consume more energy. At the same time, traffic attack is seriously harmful to WSN [6-7]. In this paper, new security schemes are proposed to revoke malicious compromised nodes with energy-saving consideration. Different kinds of nodes are monitored by different detection schemes to insure secure data aggregation.

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.

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

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

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:

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

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

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

Published by Atlantis Press, Paris, France.

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

$$T_t = \hat{\phi}_1 T_{t-1} + \hat{\phi}_2 T_{t-2} + a_t - \widehat{\theta_1 a}_{t-1} \tag{6}$$

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:

$$N_1 = \hat{\phi}_1 - \hat{\theta}_1 \tag{7}$$

$$N_2 = \hat{\phi}_2 - N_1 \hat{\theta}_1 \tag{8}$$

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

One step prediction model is as that:

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

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:

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

$$N_0 = -1 \tag{12}$$

III. Traffic Attack Detection and Secure Dada Aggregation Scheme

Since grid members only send exploratory data to grid head which participates with data forwarding, grid heads play more important roles in GDD. So electing a secure node to be grid head is important. In order to obtain secure data aggregation, it is necessary to take different monitor schemes for grid head and member nodes.

A. *Trust Evaluation by Neighbors*

After setup of grid, the grid head creates a time division schedule and informs each grid member in the same grid. Member nodes are actively transmitting or listening for a period of time and off the remainder. Member nodes transmit only at their scheduled time. This allows nodes to listen to communications in their respective grids. It is through this passive listening that member nodes are able to develop trust relationship with their neighbor nodes. Nodes that constantly drop packets or which behave in a selective or selfish manner can be easily detected by their neighbors. Each node stores and maintains a trust table and records trust values of its neighbors. As is shown in Eq.(1-3). T_i is trust value of its neighbor node i , and it is added by consistency value (C_i) and sensing communication value (S_i). Weights (W_1, W_2) are dynamic and dependent on applications. cs_i means times of collecting the same sensing data with neighbor node i, and is_i means times of collecting different sensing data. ss_i means times of sensing the same event with neighbor node i , and sf_i means times of sensing different event.

$$C_i = \frac{cs_i - is_i}{cs_i + is_i} \qquad where -1 \le C_i \le 1 \tag{13}$$

$$S_i = \frac{ss_i - sf_i}{ss_i + sf_i} \qquad where -1 \le S_i \le 1 \tag{14}$$

$$T_i = W_1 C_i + W_2 S_i \tag{15}$$

B. *Secure Grid Head Election*

When the current grid head's battery power level falls below a predetermined threshold or serves for a predetermined period of time, it broadcasts a new election message within the grid. All nodes then vote for a new grid head by using ballot. This is done by replying to the new election message with its choice of candidate. The top pick from the trust table of its neighbors is selected as the grid's candidate. At the same time, every node sends its remainder of energy to the gird head.

The current grid head then tallies the votes and decides the winner based on Eq.(16). P_j means votes of node j , while B_j means its remainder of energy. Weights (W_3 ,W_4) are dynamic and dependent on applications. If security is more important, W_3 is designed higher. If lifetime of network is critical, W_4 is designed higher. At the completion of computing, the grid head broadcasts the winner that has the highest value of Z to all the members of the grid.

$$Z = W_3 P_j + W_4 B_j \tag{16}$$

C. *Monitoring Method for Grid Head*

We add a virtual grid head in each grid to monitor grid head. The virtual grid head is elected among neighbors of grid head. Its work is to listen to grid head's input and output communications, and record traffic and wrong conclusion counts being drawn by the grid head. Once traffic or wrong counts exceeds thresholds, the virtual grid head will send a broadcast message in its grid to initiate a new round of grid head election, and the former grid head is forbidden to be elected as grid head for ever.

D. *Monitoring Method for Grid Member*

Every gird head maintains an alarm table to record the alarm messages of its grid members. The alarm table consists of two fields. The first field records the identify (ID) of the suspected grid member, and the second one takes down the alarm counts of abnormal traffic and messages. When detecting misbehavior of a grid member, grid head updates alarm messages. Once a suspected grid member's alarm counts exceed the alarm threshold, the grid head will send a broadcast message in its grid to revoke this abnormal member node, so malicious nodes are restrained.

E. *Secure Data Aggregation*

To combat failures in the reporting nodes, each node is assigned a SI , maintained at the gird head, to indicate its track records in reporting past events correctly. SI is a real number between zero and one, and it is initially set one. For each report a node makes, if that is deemed incorrect by the grid head, the node's SI is decreased. Similarly, for each report a node makes, if that is deemed correct by the grid head, the node's SI is increased, but not beyond one. Thus correctly functioning nodes will have a SI approaching one, while faulty and malicious nodes will have a low SI .

We assume that correct nodes are allowed to make occasional errors due to natural causes. The rate of these errors is denoted the natural error rate. Let the natural error rate be f_r (<1). A variable V is maintained for each node at the grid head. Each time a node makes a report deemed faulty by the grid head, then its V is increased by the expression ($1 - f_r$). Each time a node makes a report deemed correct by the grid head, then its V is decreased by f_r (if V is larger than zero). The SI is calculated as shown in Eq.(17). Where λ is a proportionality constant that is dependent on applications.

$$SI = e^{-\lambda V} \qquad (17)$$

When receiving the first sensing event report, the grid head sets up a timer. When the timer expires, according to whether reporting the sensing event, the grid head divides the nodes into two groups. When the nodes that report the sensing event are more than that do not report, the grid head accepts the sensing event, and verifies the corresponding nodes' value of V. Then the grid head aggregates the sensing data according to Eq.(18). SI_i means the trust value of nodes. SR is the aggregation result. sr_i is the data sent by nodes.

$$SR = \frac{\sum_{i=1}^{m} (SI_i + 1) sr_i}{\sum_{i=1}^{m} (SI_i + 1)} \qquad (18)$$

IV. TRAFFIC ATTACK PERFORMANCE

We take GDD as basic rooting protocol. We compare our security protocol(IPD) with another traffic attack detection protocol(ESID) designed by Su [8]. 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%.

A. *Simulation under Attacks*

1) Alive Nodes

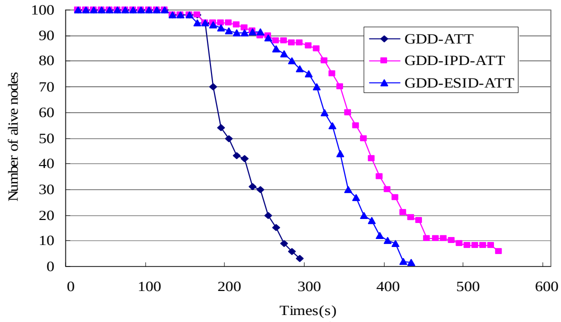

Figure 1. Number of total alive nodes

Fig. 1 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.

2)Energy Consumption

Fig. 2 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.

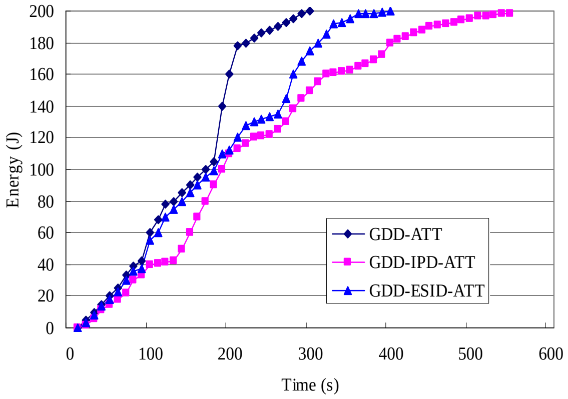

Figure 2. Node energy consumption

B. *Detection Ratio of Captured Nodes*

Fig. 3 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.

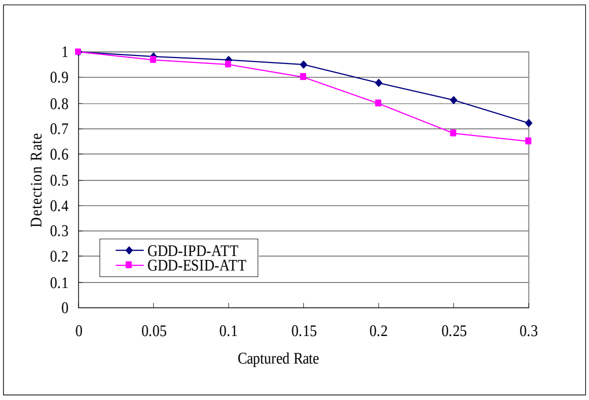

Figure3. Ratio of captured sensor nodes

Published by Atlantis Press, Paris, France.

V. SECURE DATA AGGREGATION PERFORMANCE

A. *Probability of Selecting Compromised Nodes as Grid Heads*

Table 1 shows the advantage of our secure gird head selection scheme over that does not employ our scheme. With less than 15% of compromised nodes, our scheme almost never selects a compromised node. This demonstrates the effectiveness of our scheme in electing secure grid head. However, the probability increases rapidly after 85% of the nodes are compromised. This can be explained that accumulation of errors at the node makes it increasingly difficult to discern between compromised nodes and uncompromised nodes in light of the packet drop rate and the false voting of compromised nodes.

Table Ⅰ. Probability of selecting compromised nodes as grid heads

Compromised nodes ratio (%)	**Probability(Using trust grid head election)**	**Probability(Without trust mechanism)**
0	0	0
15	0	0.2
50	0.1	0.4
85	0.2	0.8
100	1	1

B. *Data Aggregation Results*

We show the impact of nodes density and captured rate to the detection rate in Fig.4. As a whole, the detection rate is high. With increasing of node density, the detection rate increases. With increasing of captured rate, the detection rate decreases. Fig.5 shows diversification of aggregation result under different captured rates. With increasing of captured rate, aggregation result differs more from true result.

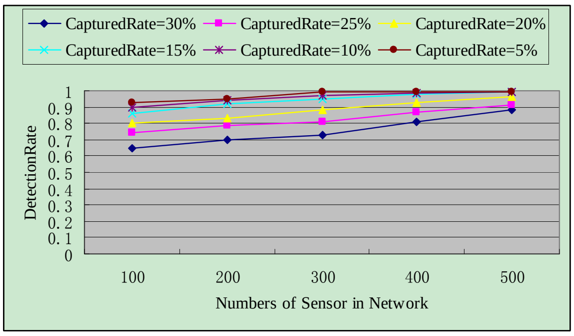

Figure 4. The impact of nodes' density and captured rate

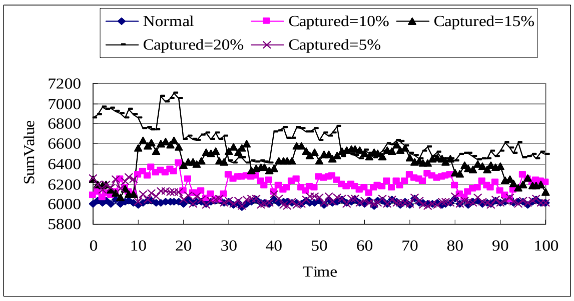

Figure 5. The impact of the captured rate

VI. CONCLUSION

In this paper, in order to adapt to secure applications, traffic attack detection and secure data aggregation schemes are added to GDD. According to different roles played by nodes, different monitor schemes are used. We use ARMA(2,1) and linear prediction technique to establish traffic prediction model. Our secure data aggregation scheme does not employ cryptographic approaches or certification schemes, so it is light enough to fit well with WSN without great overheads. Simulation shows that, our protocol is a lightweight one. It can effectively protect sensor nodes from traffic attacks, filter out false sensing data and prolong lifetime of networks.

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] Intanagonwiwat C, Govindan R, Estrin D, Heidemann J, “Directed diffusion for wireless sensor networking”, IEEE Transactions on Networking, vol. 11, pp. 2-16, 2003.

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

[3] B.T, M. H, “A Self-healing Key Distribution Scheme with Novel Properties”, International Journal of Network Security, vol. 7, pp.115-120, 2008.

[4] Rajasegarar S, Leckie C, Palaniswami M, Bezdek J C, “Distributed anomaly detection in wireless sensor netwoks”, In: 10th IEEE Singapore International Conference of Communication System, Singapore, pp.1-5, 2006.

[5] Hur J, Lee Y, Hong SM, Yoon H, “Trust-Based Secure Aggregation in Wireless Sensor Networks”, In: 3rd International Conference on Computing, Communications and Control Technologies, Austin, USA, pp.491-496, 2005.

[6] 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.

[7] 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.

[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.