International Journal of Information Technology and Knowledge Management
July-December 2010, Volume 2, No. 2, pp. 523-527

PERFORMANCE ANALYSIS OF AN OPTIMIZED ENERGY EFFICIENT DATA AGGREGATION PROTOCOL

Virender Kumar Ranga[1], Jagan Nath[2] & Mohit Dua[3]

Data aggregation in wireless sensor networks is widely accepted as an essential paradigm for energy efficient routing but with low reliability under node and link failures. Also, malicious sensor nodes send false data reports to distort aggregation results. In this paper, we propose a protocol which associates a packet's reliability in data transmission with the amount of information it contains and gives higher reliability to the packet which has more information by adjusting the degree of redundancy. It uses the concept of Functional reputation which enables data aggregators to evaluate each type of sensor node action using a respective reputation value thereby increasing the accuracy of the trust system. Therefore, this protocol can jointly optimize both information reliability and energy efficiency in sensor networks with data aggregation and improve the reliability of aggregated data in the presence of compromised nodes.
Keywords: RDA, RpF, RDAT.

1. Introduction

Wireless sensor networks consist of large numbers of resource constrained sensor nodes communicating over the wireless medium for the purpose of information gathering. Data aggregation is defined as the process of combining data from multiple sensor nodes to eliminate redundant data transmission and provide fused information to the base station. The main purpose of a sensor network is to disseminate information about the environment and the most important problem here is to deliver information correctly with less energy consumption. Accordingly, the key metric in this network is delivery reliability per energy. To attain high reliability per energy, we use redundant copies of a packet to increase its end-to-end probability of data delivery. The degree of redundancy introduced, is controlled by the amount of information the packet contains. Many wireless sensor networks are deployed in unattended hostile environments to perform mission-critical tasks and therefore security protocols are required for these networks physical security of sensor nodes cannot be provided because making sensor nodes tamper-proof is prohibitively expensive. Due to this lack of physical security, intruders can easily compromise one or more sensor nodes to subvert network operations. Compromised sensor nodes pose a challenging constraint for the protocol designer: a sensor network protocol must be highly energy efficient while being able to function securely in the presence of possible malicious compromised nodes within the network Reputation and trust concepts can be used to overcome the shortcomings of cryptography based secure and reliable data aggregation solutions. Reputation can be defined as the trustworthiness of an entity whereas trust is the expectation of one entity about the actions of another [20]. A reputation based system in wireless sensor network domain is a system in which the actions of every node are observed by the other nodes in an attempt to evaluate their trustworthiness. In this paper, effect of compromised nodes on data aggregation is mitigated using a reputation system which is built over functional reputation concept. A functional reputation of a sensor node is represented by the beta distribution of the sensor node's actions with respect to a certain function. Compared to general reputation which is computed over all actions of the sensor node, using functional reputation prevents a compromised node from covering its bad actions with respect to one function by behaving well for other functions [13]. In addition, using general reputation may affect legitimate sensor nodes in the network. For example, if general reputation is used, a legitimate sensor node that sends false sensing reports due to its malfunctioning sensing unit maybe labelled as a compromised node.

[1, 2, 3]Department of Computer Engineering, National Institute of Technology, Kurukshetra, India

Email: virender.ranga@nitkkr.ac.in[1], Jagan_nath14@rediffmail.com[2], er.mohitdua@gmail.com[3]

2. Related Works

There are extensive works on routing protocol with data aggregation. For example, Directed Diffusion [1], LEACH [2], PEGASIS [3]. The basic idea of these protocols is to construct a data aggregation tree rooting at sink to gathering data. When data delivered from sources to sink, aggregation occurs at any interaction node to eliminate the data redundancy and reduce the transmission energy. All of these approaches focus on energy aspect of data aggregation and did not consider reliability In wireless sensor network domain, secure data aggregation problem is studied extensively. In [6], the security mechanism detects node misbehaviours such as dropping or forging messages and transmitting false data. In [8], sensor nodes first send data

aggregators the characteristics of their data to determine which sensor nodes have distinct data and then those sensor nodes having distinct data send their encrypted data. Recently, trust development systems RFSN [9] and DRBTS [12] are proposed for wireless sensor networks. Both RFSN and DRBTS formulate the problem in the realm of Bayesian analytic rather than game theory. In paper [20] a protocol a novel reliable data aggregation protocol, called RDAT, which is based on the concept of functional reputation is proposed. Protocol RDA [11] which associates packet's reliability in data transmission with the amount of information it contains.

3. SYSTEM AND THREAT MODEL

We consider a large sensor network with densely deployed sensor nodes. Due to the dense deployment, sensor nodes have overlapping sensing ranges and events are detected by multiple sensor nodes. Hence, aggregation of correlated data at neighbouring sensor nodes is needed. Some sensor nodes are dynamically designated as data aggregators to aggregate data from their neighbouring sensor nodes, although every sensor node is assumed to be capable of doing data aggregation. To balance the energy consumption of sensor nodes, the role of data aggregator is rotated among sensor nodes based on their residual energy levels. Intruders can compromise sensor nodes via physical capturing or through the radio communication channel. Once a sensor node is compromised, all information of the node becomes available to the intruder. Although compromised nodes can perform many types of attacks to degrade the network's security and performance, we only consider the attacks against integrity of the aggregated data.

4. RELIABLE DATA AGGREGATION PROTOCOL

The goal of wireless sensor networks is to gathering information with high reliability and low energy, and in sensor networks with node and link failures, the reliability is usually ensured by retransmission, so we need to trade off between reliability and energy consumption, therefore, we use the metric RpE to present the system performance. RpE denotes the system reliability over the system energy consumption.

$$RpE = \text{reliability/energy} \quad (1)$$

In sensor networks with data aggregation, the information reliability is usually measured by the amount of information received by the sink over the amount of information sensed by all sources, and it is affected by two factors. One is the channel error rate and the other is the amount of information. Assume the per hop channel error rate, denoted by e ($0<e<1$), is equal, then a packet from a node h hops apart from the sink will reach the sink with probability $(1 – e)^k$ the channel error rate could be very high in sensor networks, the single-path single packet forwarding scheme cannot achieve the desired reliability. Thus, providing redundant copies with controlled redundancy degree can extremely improve the data successful arrival probability. To quantify the amount information generated by sources and by aggregation points after compression, we use the entropy H of a source to denote the amount of information it originates. Here, we model the average joint entropy of n sources, Hn, as a function of inter-source distance d, we have:

$$Hn(d) = H1 + (n – 1)[1 – (1/(d/c + 1)]H1 \quad (2)$$

where c is a constant that characterizes the extent of spatial correlation between the data. It is chosen such that when c = d, H2 = 3/2H1 i.e. the second source generates half the first node's amount in terms of uncorrelated data. To quantify the energy expenditure, we use the model discussed in [11]. We assume each node uses fixed energy for 1-bit data transmission. Suppose when transmit a 1-bit packet a node needs Eelec to run the transmitter or receiver circuitry and 0.5 E elec for the transmitter amplifier. The transmission cost and receiving cost for a k " bit message is:

- Transmission:

  $ETx(k) = Eelec \times k + 0.5\times Eelec \times k$

- Receiving:

  $ERx(k) = Eelec \times k$

  The total for deliver k – bit message is:

  $E(k) = ETx(k) + ERx(k) = 2.5 \times Eelec \times k$

We let $Ec = 2.5 \times Eelec$ in that way, the cost of deliver k – bit message is

$$E(k) = Ec \times k \quad (3)$$

For jointly optimizing both information reliability and energy efficiency, the objective of this problem is to give suitable redundancy degree to each packet in order to maximize the reliability per energy.

To evaluate trustworthiness of sensor nodes by using three types of functional reputation, namely sensing, routing, and aggregation. Sensor nodes monitor their neighbourhood to obtain first-hand information regarding their neighboring nodes. For sensing, routing, and aggregation tasks, each sensor node Ni records good and bad actions of its neighbors in a table referred to as functional reputation table. Functional reputation tables are exchanged among sensor nodes to be used as second-hand information during trust evaluation. The functional reputation tables are piggy backed to other data and control packets in order to reduce the data transmission overhead. When sensor node Ni needs to interact with its neighbour Nj, Ni evaluates the trustworthiness of Nj using both first-hand and second-hand information regarding Nj. Functional reputation for aggregation ($R_{i,j}^{aggregation}$) is needed by sensor nodes to evaluate the trustworthiness of data aggregators. Functional

reputations for routing ($R_{i,j}^{routing}$)and sensing ($R_{i,j}^{sensing}$) are used by data aggregators to increase the security and reliability of the aggregated data. Functional reputation values are quantified using beta distributions of node actions.

(A) Computing Functional Reputation and Trust

Functional reputation value ($R_{i,j}^{X}$) is computed using beta density function of sensor node Nj's previous actions with respect to function X. Trust ($T_{i,j}^{X}$) is the expected value of $R_{i,j}^{X}$.Let us take routing task as an example. If sensor node Ni counts the number of good and bad routing actions of Nj as α and β, respectively. Then, Ni computes the functional reputation $R_{i,j}^{routing}$ about node Nj as Beta(α+1, β+1). Following the definition of trust, $T_{i,j}^{routing}$ is calculated as the expected value of $R_{i,j}^{routing}$

$$T_{i,j}^{routing} = E(Beta(\alpha+1, \beta+1))$$
$$= \alpha+1/\alpha+\beta+2$$

This equation shows that the expected value of the beta distribution is simply the fraction of events that have had outcome á. Hence, functional reputation value of routing is given by the ratio of good routing actions to total routing actions observed. This is an intuitive decision and it justifies the use of the beta distribution. In the above formula, $R_{i,j}^{routing}$ represents node Ni's observations about node Nj. In other words, it just involves first-hand information. Reputation systems that depend on only first-hand information has a very large convergence time. Hence, second-hand information is desirable in order to confirm firsthand information. In protocol RDAT, neighbouring sensor nodes exchange their functional reputation tables to provide second-hand information and this information is included in trust evaluation. Let us assume that sensor node Ni receives second-hand information about node Nj from a set of N nodes and $S_{info}(r_{k,j})$ represents the second-hand information received from node Nk (k N). Ni already has previous observations about Nj as $\alpha_{i,k}$ and $\beta_{i,j}$. Further assume that, in a period of Δt, Ni records $r_{i,j}$ good routing actions and $s_{i,j}$ bad routing actions of Nj. Then, Ni computes the trust $T_{i,j}^{routing}$ for N_j as follows.

$$\alpha_{i,j}^{routing} = \nu*\alpha_{i,j} + r_{i,j} + \Sigma S_{info}^{routing}(r_{k,j})$$

$$\beta_{i,j}^{routing} = \nu*\beta_{i,j} + r_{i,j} + \Sigma S_{info}^{routing}(r_{k,j}) \quad T_{i,j}^{routing} = E(beta(\alpha_{ij}routing + 1, \beta_{ij}^{routing} + 1))$$

where $\nu < 1$ is the aging factor that allows reputation to fade with time. Integration of first and second hand information into a single reputation value is studied in by mapping it to Dempster-Shafer belief theory . We follow a similar approach and use the reporting node Nk's reputation to weight down its contribution to the reputation of node Nj. Hence, second-hand information $S_{info}(r_{k,j})$is defined as

$$S_{info}(r_{k,j}) = (2*\alpha_{i,k} * r_{k,j})/((\beta_{i,k} + 2) * (r_{k,j} + s_{k,j} + 2) * (2 * \alpha_{i,k}))$$

$$S_{info}(s_{k,j}) = (2*\alpha_{i,k} * s_{k,j})/((\beta_{i,k} + 2) * (r_{k,j} + s_{k,j} + 2) * (2 * \alpha_{i,k}))$$

The idea here is to give greater weight to nodes with high trust and never give a weight above 1 so that second-hand information does not outweigh first-hand information. In this function, if $\alpha_{i,k} = 0$ the function returns 0, therefore node Nk's report does not affect the reputation update.

(B) Secure and Reliable Data Aggregation

In this protocol, data aggregation is periodically performed in certain time intervals. Time is divided into epochs, where a single data aggregation process takes place. In each data aggregation session, secure and reliable data aggregation is achieved in two phases. In the first phase, before transmitting data to data aggregators, each sensor node Ni computes $R_{i,j}^{aggregation}$ value for its data aggregator Aj and evaluate the trustworthiness of Aj. If trustworthiness of Aj is below a predetermined threshold, then Ni does not let Aj to aggregate its data. To achieve this, Ni encrypts its data using the pair wise key that is shared between the base station and Ni and sends this encrypted data to the base station along with a report indicating Aj may be compromised. Based on the number of reports about Aj over the time, the base station may decide that Aj is a compromised node and it should be revoked from the network. In the second phase of data aggregation session, the following algorithm is run by data aggregators. Algorithm RDA depends on $R_{i,j}^{sensing}$ and $R_{i,j}^{routing}$ functional reputation values to mitigate the effect of compromised sensor nodes on aggregated data.

Algorithm

- Input: Data aggregator Aj, Aj's neighboring nodes {N1, N2, ..., Ni}, trust values of neighboring nodes computed by Aj {$T_{j,1}^{sensing}$,..., $T_{j,i}^{sensing}$} and {$T_{j,1}^{routing}$,..., $T_{j,i}^{routing}$}.
- Output: Aggregated data Dagg.
- Step 1: Aj requests each Ni to send its data for data aggregation.
- Step 2: Sensor nodes {N1, N2, ...,Ni} transmit data {D1, D2, ...,Di} to Aj.
- Step 3: Aj updates trust values $T_{i,j}^{sensing}$ and $T_{i,j}^{routing}$ of each Ni based on the first and second hand information regarding Ni.
- Step 4: when Aj receives data packet

If (this packet is never received before) Then
{
Aj weights data Di of sensor node Ni using the $T_{i,j}^{sensing}$

and $T_{i,j}^{routing}$

H1= the amount of information
a source senses;

Hk= the amount of information
after aggregation;

$\alpha = (1/(1 - e))$

$p = \alpha * (Hk/H1)$

Aj aggregates the weighted
data to obtain Dagg.
}

- Step5: If (all packets from children
  received or this round is
  over)Then
  {
  Send the aggregation
  packet to parent p times;
  }

Since compromised nodes send false sensing reports in order to deceive the base station, Algorithm considers trustworthiness of sensor nodes with respect to sensing function to increase the reliability of aggregated data. To achieve this, Aj weights data of each sensor node Ni with respect to the sensor node's trust value $T_{i,j}^{sensing}$ and $T_{i,j}^{routing}$. By weighting sensor data based on trust levels, data aggregators reduce the compromised sensor nodes' effect on the aggregated data.

4. RESULTS

With the simulation result, it can be shown that the protocol implemented in this paper is novel reliable data aggregation and more energy efficient protocol and less error rate than previous implemented protocol.

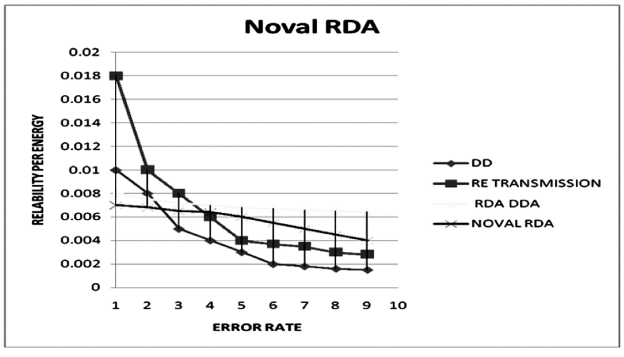

Fig. 1: Reliability Vs. Error Rate

5. CONCLUSION AND FUTURE WORK

This paper has presented a novel reliable data aggregation and transmission protocol that uses the functional reputation concept. It can jointly optimize both information reliability and energy efficiency in sensor networks with data aggregation. In comparison with other protocols improved reliable data aggregation protocol improves the security and reliability of the aggregated data .though this protocol improves the security, yet it does not address the problem of denial of service (dos) attack and this is the area that will form part of our future work.

REFERENCES

[1] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks.", IEEE/ACM Transactions on Networking, 11, No. 1, Feb. 2003, pp. 2–16.

[2] Lindesy S, Raghavendra C S. "PEGASIS: Power Efficient Gathering in Sensor Information Systems." Proceedings of IEEE Aerospace Conference, Big Sky, MT, Mar. 2002.

[3] Wendi B. Heinzelman, Anantha P. Chandrakasan,, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks" IEEE Transactions on Wireless Communications, Oct. 2002.

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, 40(8), pp. 102 -114, Aug. 2002.

[5] R. Rajagopalan and P.K. Varshney, "Data Aggregation Techniques in Sensor Networks: A Survey", IEEE Communications Surveys and Tutorials, 8, No. 4, 4th Quarter 2006.

[6] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks", IEEE Comp. Mag., Oct. 2003, pp. 10305.

[7] H. C¸ am, S. Ozdemir, P. Nair, and D. Muthuavinashiappan, and H.O. Sanli, "Energy-Efficient and Secure Pattern based Data Aggregation for Wireless Sensor Networks", Special Issue of Computer Communications on Sensor Networks, pp. 446-455, Feb. 2006.

[8] W. Du and J. Deng and Y. S. Han and P. K. Varshney, "A Witness-Based Approach for Data Fusion Assurance in Wireless Sensor Networks", in Proc. of GLOBECOM '03, pp. 1435-9, 2003.

[9] S. Ganeriwal and M. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks", in Proc. of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks, October 2004 pp. 66-77.

[10] R. Rajagopalan and P.K. Varshney, "Data Aggregation Techniques in Sensor Networks: A Survey", IEEE Communications Surveys and Tutorials, 8, No. 4, 4th Quarter 2006.

[11] Hong Luo, Qi Li, Wei Guo, "RDA: Data Aggregation Protocol for WSNs", Beijing Key Laboratory of Intelligent Telecommunications Software and Multimedia, IEEE2006 (p 1-4).

[12] A. Srinivasan, J. Teitelbaum and J. Wu, "DRBTS: Distributed Reputation based Beacon Trust System", In the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC06), Indianapolis, USA, 2006.

[13] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks", Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, A. Boukerche (ed.), Wiley and Sons, 2008.

[14] M. Raya, P. Papadimitratos, V.D. Gligor, and J.P. Hubaux. "Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks", Proc. of INFOCOM, pp. 1912-1920, 2008.

[15] S. Ozdemir, "Secure and Reliable Data Aggregation for Wireless Sensor Networks", LNCS 4836, H. Ichikawa et al. (Eds.), pp. 102-109, 2007.

[16] A. Josang and R. Ismail, "The Beta Reputation System", Proc. 15th Bled Conf. Electronic Commerce, 2002.

[17] I. S. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields", SIAM Journal of Applied Math, 8, pp. 300304, 1960.

[18] K. Wu, D. Dreef, B. Sun, and Y. Xiao, "Secure Data Aggregation without Persistent Cryptographic Operations in Wireless Sensor Networks", Ad Hoc Networks, 5, No.1, pp. 100-111, 2007.

[19] Suat Ozdemir, "Functional Reputation based Data Aggregation for Wireless Sensor Networks", IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, 2008.

[20] Tamara Pazynyuk, JiangZhong Li, George S. Oreku, "Reliable Data Aggregation Protocol for Wireless Sensor Networks", IEEE, 2008.