A Secure Energy Efficiency Routing Approach in Wireless Sensor Networks

M.Sri Lakshmi[1], Meda Ramya Sai[2], Yeruva Lakshmi[3]
Department of Computer Science and Engineering
[1]Assistant Professor, G.Pullaiah College of Engineering and Technology, Kurnool.
[2, 3] B.Tech G.Pullaiah College of Engineering and Technology, Kurnool.

Abstract-*For the energy limited wireless sensor networks, the critical problem is how to achieve the energy efficiency. Many attackers can consume the limited network energy, by the method of capturing some legal nodes then control them to start DoS and flooding attack, which is difficult to be detected by only the classic cryptography based techniques with common routing protocols in wireless sensor networks. We claim that under the condition of attacking, existing routing schemes are low energy-efficient and vulnerable to inside attack due to their deterministic nature. To avoid the energy consumption caused by the inside attack initiated by the malicious nodes, this paper proposes a novel energy efficiency routing. Under our design, each node computes the trust value of its 1-hop neighbors based on their multiple behaviors attributes evaluation and builds a trust management by the trust value. By this way, sensor nodes act as router to achieve dynamic and adaptive routing, where the node can select much energy efficiency and faithful forwarding node from its neighbors according to their remaining energy and trust values in the next process of data collection.*

Keywords*-*Wireless Sensor Networks, Sensor Nodes, Local Trust Management Mechanism.

I. INTRODUCTION

Wireless sensor networks is a kind of self-organized network based on wireless communication technology, for the purpose of cooperate apperceiving, collecting and dealing the information of the objects in the covered geographic area and transmitting to the sink node after data process [1–4]. The appearance of Wireless sensor networks is not only helpful for realizing the conception of ubiquitous computing, but also for promoting the interaction between human and physical world. Wireless is not only helpful for realizing the conception of ubiquitous computing, but also for promoting the interaction between human and physical world. Special in the unmanned wild field or enemy field, various possible threats come during the process of data collection. Hence, it is important to protect the resource as Wireless sensor networks is easier to be attacked.

As most of sensor nodes are unable to communicate with the sink node directly for their limitation of communication capacity, the method of direct transmission is hardly to meet the needs of large deployment. Hence, the data collection is completed by the multi-hop transmission in Wireless sensor networks. For these compromised nodes, their legal identity make them freely send data [5, 6]. At the same time, other nodes after receiving these data need to proceed and retransmit. Hence, attackers can use these compromised nodes to create some meaningless or fake information and consume the energy of normal nodes by DoS or flooding method [7, 8].

This paper is focus on how to guarantee the energy efficiency when the inside attack occurs, it has obvious uniqueness and complexity. Firstly, wireless sensor networks consist of a large number of sensor nodes so the price of sensor node should be as low as possible. Secondly, multi-hop is adopted in Wireless sensor networks, which make the network easier to be eavesdropped or interrupted than cable network. Thirdly, the attacker can insert error data to mislead the network which can rapidly run out of the network energy. The main contributions of this paper are summarized as follows:

We analyze the abnormal behavior model when the network is attacked from inside side and calculate derivation of trust value. Then we propose a local trust management scheme based on the trust value of neighbor nodes, which can be used to the reliability of nodes measure.

The rest of this paper is organized as follows. Section 2 presents some related works. Section 3 introduces the system model and gives the problem statement and the inside attack is analyzed and local trust management scheme is presented. Finally, summarizes our work and concludes the paper.

II. SYSTEM STUDY

2.1 WSN ARCHITECTURE

In a typical WSN we see following network components –

- Sensor motes (Field devices) – Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.
- Gateway or Access points – A Gateway enables communication between Host application and field devices.
- Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.
- Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

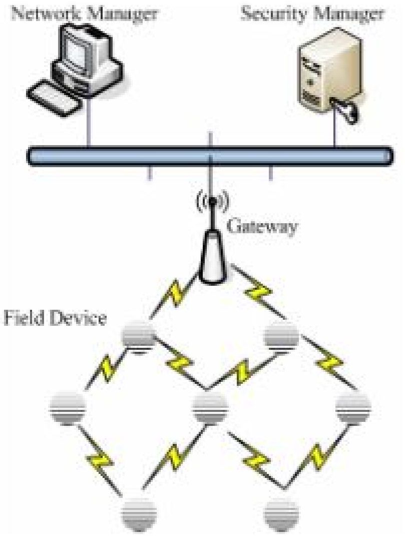


Figure 1. WSN Architecture

2.2 System Model and Problem Statement

Network Models and Assumptions

We consider a wireless sensor network composed of moderately large number of resource constrained sensor nodes, denoted by n1, n2, n3 ……., nn. We further assume that the sensor nodes are deployed in high density. These nodes are used for data collection in the monitoring area. Each Sensor nodes has a communication range such that if the distance between two sensors is more than this range, they are not communicating. Without loss of generality, we make the following considerations in this paper:

- All the sensor nodes and the sink node do not move after the deployment Except for the sink node, all the sensor nodes are isomorphic with the same initial energy, computation capacity, and data fusion capacity.
- According to the distance to the receiver, the sensor nodes can adjust the transmission power to save energy consumption.
- The links are symmetrical. If the transmission power of the opposing side is known, the sensor nodes can calculate the approximate distance to the sending node from the signal intensity of the receiving signal.

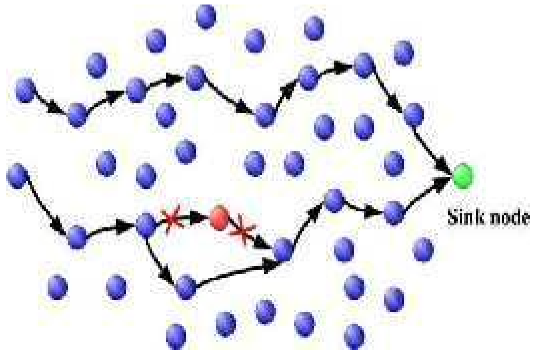


Figure 2: Example of avoiding the compromised nodes

Since the sink node interface a wireless sensor network to the outside world, the compromise of it can render the entire network useless. For this reason we assume that the sink node are trustworthy, in the sense that they can be trusted and assumed to behave correctly.

Problem Description

For the limited communication ability, most of sensor nodes are unable to communicate with the sink node directly. Therefore, these nodes need to find some forward nodes which can relay their sensory data to the sink node. In this case, how to improve the energy efficiency during routing establishment in Wireless sensor networks is very necessary. Once a node is compromised, the attackers are always acquire the encryption/decryption keys of that node, and thus can intercept any information passed through it. Additionally, the attackers can start DoS and flooding attack by these compromised nodes to consume the energy of normal mode.

Our purpose is to improve the energy efficiency routing with node compromised resistance [17]. To achieve this we purpose, each node need to proceed trust management on all the neighbor nodes. Each node has multiple properties, and the nodes for inside attack have obvious difference in behavior to other ordinate node, such as tempering the data packet, blocking and delaying the data transmission. In this way the behavior difference can be used to detect the malicious node.

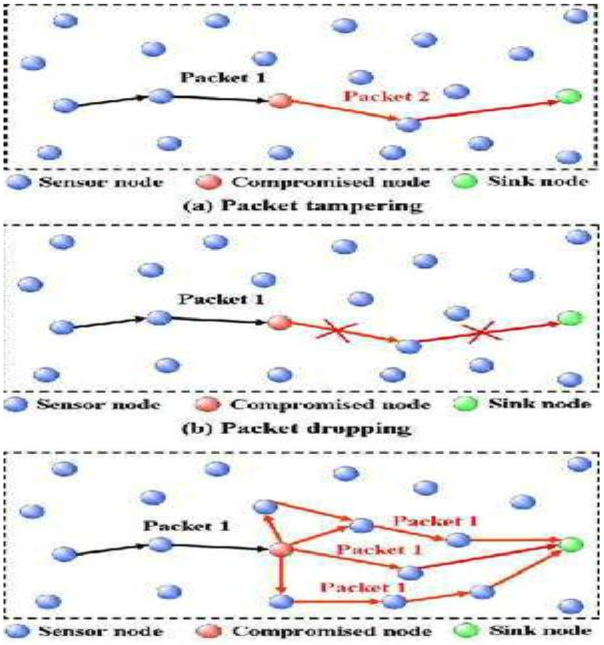
III. LOCAL TRUST MANAGEMENT MECHANISM

In this we analyze the damage of inside attack and the behavior model of compromised node. Based on the monitoring abnormal behavior of neighbor node, herewith we propose a local trust management mechanism, which can be used to detect the compromised node by low energy consumption.

3.1Analysis of Insider Attack in Wireless Sensor Networks

Based on the knowledge and privileges of the adversary, we can divide the attacks into two kinds: one is outside attack processed by outside nodes without legal identity, the other is the inside attack processed by the nodes with legal identity [14].

To compromise a sensor node over the wireless channel, an adversary can exploit weaknesses in software implementation, the applied protocols, and even the security protocols with incorrectly implemented in protocol design. All this above might enable the adversary to access secret data by sending messages that are non-compliant to the protocol. After a node is compromised, an adversary has knowledge of all data stored on the node, such as the program code and cryptographic keys. Figure 2 describes three kinds of attack, including packet tamper, packet drop and packet flood. Furthermore, several compromised sensor nodes may plot and exchange data, e.g., they may exchange cryptographic keys using an out-of-band channel and then collaboratively perform an attack. The most difficulty and the precondition to resist the inside attack is how to find those compromised nodes.



(a) Packet tampering

(b) Packet dropping

Figure 3: Example of Attack

3.2 Trust Management Model

As mentioned above, sensor nodes can be compromised and the severe resource constraints exacerbate the use of the strong cryptographic mechanisms and protocols [15], which results in prevention of inside attacks is hard to achieve. To establish a trust management model, the constituent element should be clearly known, which is directly related to the definition of trust. As there is obvious difference during various trust definitions, the evaluation of trust to node generally consists of several parts:

Communication behavior: During data collection, the compromised nodemight distort the transmitted data package or send the unnecessary data package. Hence, the compromised node can be classified by observing the communication behavior. For example, if a node can correctly resend the data in time, this can be considered as trust node with increasing the trust value. Otherwise, the trust value will be reduced.

Data process: Sensor node will gather data according to the application, andthen transmit to the information server by sink node. To reduce the information amount, transmission energy consumption and storage requirement, data aggregation, also named as data fusion is used. In these data process, the trust management can improve the fault-tolerant ability of system, identify the error information, and increase the data accuracy.

3.3 Minimum Energy Function

This function investigates the minimum energy function of the cell partitioned network under consideration. In our network model, each user either uses zero power or full power [9]. Furthermore, packets can be transmitted from the sender to the receiver in the same (adjacent) cell if the sender uses full power. Furthermore, R1(R2) packets can be transmitted from the sender to the receiver in the same(adjacent) cell if the sender uses full power.

The minimum energy function$\Phi(\lambda)$ is defined as the minimum time-average energy required to stabilize an input rate λ per user, considering all possible scheduling and routing algorithms that conform to the given network structure [10]. We exactly compute this function for our network model. Specifically, we assume that all users receive packets at the same rate i.e., $\lambda i = \lambda$ for all.In this work, we restrict our attention to network control algorithms that operate according to the given network structure described above. A general algorithm within this class will make scheduling decisions about what packet to transmit, when, and to whom. For example, it may decide to transmit to a user in an adjacent cell rather than to some user in the same cell, even though the transmission rate is smaller. However, we assume that the packets themselves are kept intact and are not combined or network coded[15].

IV. OBSERVATIONS

Study and Analysis of the above algorithms have been conducted implemented to calculate the capacity of the network. The energy consumed by each network is also calculated for these algorithms. Following results have been observed during complete analysis:

- The delay of the Trust Management Model is analyzed using this procedure. This delay bound specifically, we first evaluate bounds on the expression by computing the steady-state service rates which is achieved by the Minimum Energy Algorithm.
- In the Minimum Energy Function,the numbers of routing packets are reduced, so that the energy for all nodes in networks can be efficiently used.
- Minimum Energy algorithm is developed to save energy consumption of nodes. This system delivers more than 95% of the packets with low end-to-end delay, but it fails to specify the loss of packets.

V. CONCLUSIONS

In this chapter, we presented a novel energy efficiency routing with node compromised based on trust management model in Wireless sensor networks. In trust management, each node needs to record and manage the remaining energy information and trust value of its neighbor nodes. The trust value is computed based on the multiple behavior attributes. One advantage of trust management is that, it is a dynamic and adaptive routing. The established routing from the source node by trust management to the sink node can combine the energy efficiency and security of data transmission. The compromised node can be detected and avoided to prevent the attacked energy consumption. The trust management indicates the high performance in energy-efficient and combating inside attack from the compromised nodes.

REFERENCES

[1] K. Lin, C-F Lai, (2012) Dalian Univ. of Technology, Dalian, Liaoning, China.

[2] Chen M, Leung V, Mao S, Yuan Y (2007) DGR: directional geographical routing for real-time video communications in wireless sensor networks. Elsevier Computer Communication 30(17):3368–3383.

[3] Lin K, Wang L, Li K, Shu L (2010) Multi-attribute data fusion for energy equilibrium routing in wireless sensor networks. KSII Trans Internet Information Systems 1(1):5–24.

[4] Chen M, Leung V, Mao S, Kwon T (2009) RLRR: receiver- oriented load-balancing and reliable routing in wireless sensor networks. Wireless Communication Mobile Computer 9(3):405–416.

[5] Lin K, Chen M, Ge X (2010) Adaptive reliable routing based on cluster hierarchy for wireless multimedia sensor networks. EURASIP J Wireless Communication Network 341–349.

[6] Peng M, Xiao Y, Chen H, Hao Q, Vasilakos AV, Wu J (2010) Sensor distribution on coverage in sensor networks. QShine.

[7] Fan Q, Wu Q, Magoules F, Xiong N, Vasilakos AV, He Y(2009) Game and balance multicast architecture algorithms for sensor grid. Sensors 9:7177–7202.

[8] Chen M, Kwon T, Yuan Y, Choi Y, Leung V (2007) MADD: mobile-agent-based directed diffusion in wireless sensor networks. EURASIP J Application Signal Process 2007(1):219–242.

[9] Duy Ngoc Pham, HyunseungChoo, (2008) “Energy Efficient Ring Search for Route Discovery in MANETs”, IEEE ICC.

[10] P. G. V. SURESH KUMAR,SEELAM SOWJANYA,” DEVELOPING AN ENTERPRISE ENVIRONMENT BY USING WIRELESS SENSOR NETWORK SYSTEM ARCHITECTURE”. International Journal of Computer Engineering In Research Trends.,vol.2,no.10,pp.902-908,October 2015.

[11] D.J. Ashpin Pabi, N.Puviarasan, P.Aruna,” Fast Singular value decomposition based image compression using butterfly particle swarm optimization technique (SVD-BPSO),” International Journal of Computer Engineering In Research Trends.,vol.4,no.4,pp.128-135,April 2017.

[12] Kumara Swamy , E Ramya,” A Contemplate on Vampire Attacks in Wireless Ad-Hoc Sensor Networks”, International Journal of Computer Engineering In Research Trends.,vol.2,no.12,pp.834-836,December 2017.

[13] Priya Manwani, Deepty Dubey,” Hybrid Protocol for Security Peril Black Hole Attack in MANET”, International Journal of Computer Engineering In Research Trends.,vol.3,no.3,pp.92-97,March 2017.