A Secure Energy Efficiency Routing Approach in Wireless Sensor Networks

Anuradha Garg, Ajay Tiwari, Hemant Kumar Garg

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 argue 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 Network, Energy efficiency, node compromised, trust management.

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. Wireless sensor networks are of fascinating potential application in military, medical care, commerce, education, environment and other fields. For they are equipped with heap batteries for power supply, energy efficiency is very important and a great challenge in the expectation of surviving network for a long period. 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.

Manuscript received on February 13, 2013.

Anuradha Garg, Astt. Prof., Alankar PG Girls College, Jaipur, India.
Dr.Ajay Tiwari, Astt. Prof., Tirupati College of Technical Education, Jaipur, India.
Hemant Kumar Garg, Lecturer, Govt. Women Polytechnic College, Jaipur, India.

In this process, the most importance and the key focus is to establish a reasonable routing to achieve the energy efficiency. During data collection, the unreliable wireless channels and unattended operation make sensor nodes very easy to be compromised, which result in disrupt normal data delivery between source nodes and the sink. 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. Therefore, these nodes are resource restrained in terms of energy supply, computing, storage, and communication bandwidth, which make the high complexity of security mechanism difficult be adopted in Wireless sensor networks. 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. In Section 4, the inside attack is analyzed and local trust management scheme is presented. In Section 5 we present trust management model. Finally, summarizes our work and concludes the paper.

II. RELATED WORKS

With the universal application of sensor networks, it is attracting more and more attentions to use the limited energy more efficiently and guarantee its normal work under unsafely environment. It is a complex problem about the establishment of routing which can resist the attack should have higher energy efficiency. Currently, the relative research includes energy efficient routing mechanism, security detection and evaluation, key management, and the security routing for specific attack. With the continuously occurring of new attacks, more and more researches on attack detection and evaluation method are developed. The main purpose

of these studies is to detect what kind of attack or the network situation after being attacked. The attack detection is focused on one or more kinds of attacks.

III. SYSTEM MODEL AND PROBLEM STATEMENT

A. *NETWORK MODEL AND ASSUMPTIONS*

We consider a wireless sensor network composed of moderately large number of resource constrained sensor nodes, denoted by n1, n2, n3 ……., n_n. 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. Each sensor node has a unique identification mark. The sink node is not limited by energy and computation 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.

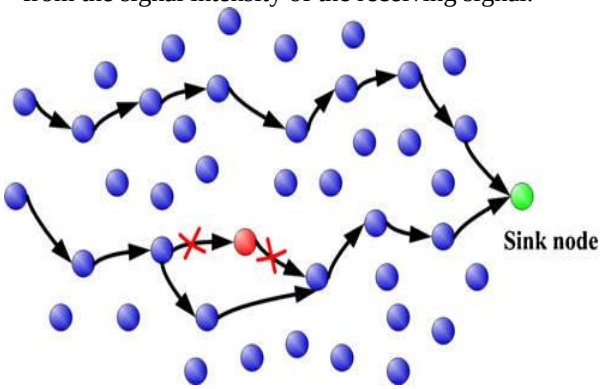

Figure 1: Example of avoiding the compromised nodes

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. As Wireless sensor networks use wireless communications, we assume that radio links are insecure. Attackers can eavesdrop on the radio transmissions, inject false data in the channel, and resend previously heard packets. We further assume that the sensor nodes can be compromised by attackers. When an adversary compromises a sensor node, it can extract all key material, data, and code stored on that node.

B. *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. Specially, data transfer process will encounter many kinds of security threatens, wherein node compromised attack is the most famous and difficult to defend against. 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. The thought of which is to willingly escape the compromise nodes during the data collection. To achieve this 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.

IV. 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.

A. *Analysis of Insider Attack In Wireless Sensor Networks*

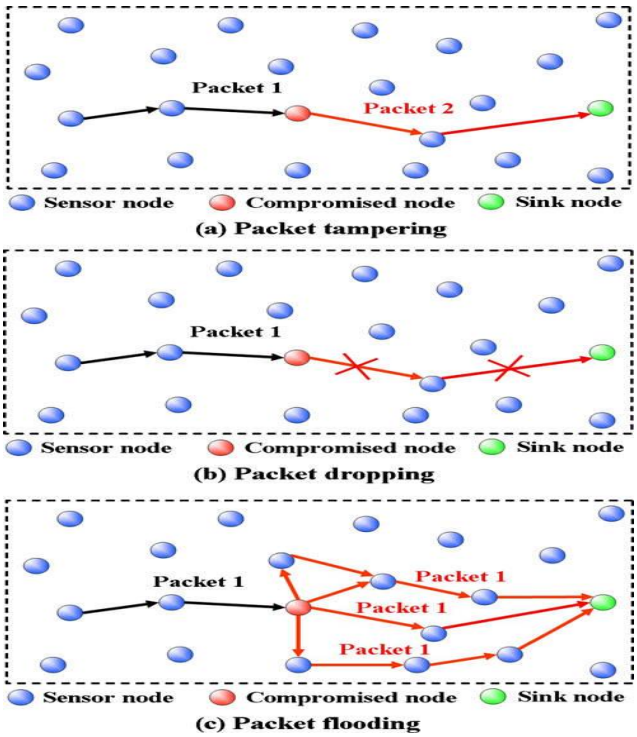

Figure 2: Example of Attack

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. Here, the inside attack is much difficult to be defended than outside attack and it can be launched from either compromised sensor nodes or from adversaries using stolen key material, code, and data from legitimate nodes. Node compromising is the most dangerous and realistic threat of inside attack since sensor nodes may be deployed in unattended or even hostile environments and usually are not tamper-resistant. It can be performed either by physically accessing the sensor node or over the wireless channel. For attacks based on physical access, if sensor nodes in certain scenarios are equipped with tamper-resistant hardware, then the attack ranges from simply connecting a laptop to a programming interface of the sensor node to sophisticated side channel attacks. For side channel attacks, it is well known that an adversary applies techniques such as manual micro probing, laser cutting, glitch attacks, or power analysis, to extract protected software and data from the smartcard processor. 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. Using these data, an adversary can perform subsequent inside at tacks. By reprogramming a sensor node, an adversary is able to launch more sophisticated attacks, such as data alteration, message negligence, selective forwarding, jamming, and special for DoS and flooding method on energy consumption, etc. 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. This represents that an inside adversary can cause much more damage than an outside adversary. The most difficulty and the precondition to resist the inside attack is how to find those compromised nodes.

B. 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, which results in prevention of inside attacks is hard to achieve. The saved information might be exposed if the node is compromised, which is a big threaten to traditional cryptographic system. It is necessary to consider how to make the network run in normal even when some of the nodes are compromised. We focus on designing the local trust management mechanism, which can distinguish the compromised node from the normal nodes. Combing the trust management and routing technology, the safety and viability of Wireless sensor networks can be improved.

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 node might 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. As it is high energy consumption when the node is continuously in monitoring state, hence, the destination nodes need to reply when they receive data packages so that all the nodes in the routing and source node can verify the reply and evaluate the node. Additionally, the number of sent data package can be recorded. If the number is over the upper limit, Dos or flooding attack might occur. If the number is not arrive the lower limit, some data might be abandoned.
- **Key mechanism:** Key mechanism is one of the important factors in many trust management system. The most usual method is to increase the trust value when the authorized node cannot decode the content in data package. The opposite is the same. By message authentication code (MAC), the trust can be improved. In hash chain system, if the current hash value is not deduced, the trust value will be reduced. If the current hash value is derivable but apart from the last hash value, it can be considered that the data is loss in transmission. According to the interval in hash chain, the trust value should be reduced.
- **Data process:** Sensor node will gather data according to the application, and then 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. The credibility of data can be classified into whether some events happened and the consistence of reported data. Special for judging the consistence, it can be considered with data fusion technology.

In our work, we observed behavior of sensor node includes all the above elements. For those compromised sensor nodes, they exhibit different behavior with other normal nodes. The trust value can be calculated from derivation degree of sensor node behavior. To facilitate this, we set N(t) as neighbors of node t and define $b_j(v)$ as j-th behavior attribute of the neighbor node v. The trust value T(v) can be calculated according to the degree of divergence from the neighborhood activities. To standardize each behavior attribute, we set μ_j and σ_j respectively, as sample average and standard deviation of the j-species behavior attribute of the neighbor node v. For each node, the first standardizes the j-th behavior attribute of its neighbor node v and computes the absolute value dj(v) by Equation 1.

$$d_j(v) = p_j | b_j(v) - \mu_j / n_j | \quad (1)$$

Where p_j denotes weight factor of j-*th behavior at* tribute. Sensor t can find the sum of behavior attributes $D(v) = d_j(v)$, which indicated the total of deviation from the neighborhood activities. Then the trust value of node v can be calculated by Equation 2. Each sensor node needs to save the trust values of all neighbor nodes and renew the

monitoring results. Compared to global management, the trust management can greatly reduce the energy consumption for exchanging information, which is more benefit for sensor network.

$$T(v) = D_{min}/D(v) \quad (2)$$

We design the local trust management model, which each node only maintains the trust value of its neighbor node. To measure the reliability of node, the behavior of neighbor node can be acquired during data gathering and the corresponding evaluation can be obtained. Besides of direct monitoring object node, the indirect information is another important content in trust value computing.

V. CONCLUSIONS

In this paper, 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. Spyropoulos T, Rais R, Turletti T, Obraczka K, Vasilakos AV (2010) Routing for disruption tolerant networks: taxonomy and design. Wireless Network 16(8):2349–2370.
10. Chen M, Leung V, Mao S, Xiao Y, Chlamtac I (2009) Hybrid geographical routing for flexible energy-delay tradeoffs. IEEE Trans Veh Technology 58(9):4976–4988.
11. Chen M, Kwon T, Choi Y (2006) EDDD: energy-efficient differentiated directed diffusion (EDDD) for real-time traffic in wireless sensor networks. Elsevier Computer Communication 29(2):231–245.
12. Chen M, Leung V, Mao S (2009) Directional controlled fusion in wireless sensor networks. Mobile Network Application 14(2):220–229.
13. Chen M, Gonzalez S, Leung V (2007) Applications and design issues of mobile agents in wireless sensor networks Wireless Communication Management 14(6):20–26.
14. Giridhar A, Kumar PR (2005) Maximizing the functional lifetime of sensor networks. In: Proceedings of the 4th international conference on information processing in sensor networks (IPSN), pp 5–12.
15. Li J, Mohapatra P (2007) Analytical model and mitigation techniques for the energy hole problems in sensor networks Pervasive Mobile Computer 3(8):233–254.
16. Powell O, Leone P, Rolim J (2007) Energy optimal data propagation in wireless sensor networks. J Parallel Distributing Computer 67:302–317.
17. Efthymiou C, Nikoletseas S, Rolim J (2006) Energy balanced data propagation in wireless sensor networks. Wireless Network 12:691–707.
18. Mhatre V, Rosenberg C (2004) Design guidelines for wireless sensor networks: communication, clustering and aggregation. Ad Hoc Networks 2:45–63.
19. Wood A, Stankovic J (2002) Denial of service in sensor net works. IEEE Computer 35(10):54–62.
20. Douceur J (2002) The sybil attack. In: Proc. of first international workshop on peer-to-peer systems (IPTPS'02). LNCS 2002, vol. 2429. Cambridge, MA, USA, pp 251–260.
21. Hu Y, Perrig A, Johnson U (2002) Wormhole detection in wireless ad hoc networks. Department of Computer Science, Rice University Tech. Rep. TR01-384.