Defence of Trust Management Sensing Based on Secure Routing Mechanism for Wireless sensor Networks

DR. R.VIJAYARAJESWARI[1], RAM SUGEERTHI[2]

[1, 2] *Department of Computer Science and Engineering, Mahendra Engineering College, Namakkal*

Abstract- Aiming at the serious impact of the typical network attacks caused by the limited energy and the poor deployment environment of wireless sensor network (WSN) on data transmission, a trust sensing based secure routing mechanism (TSSRM) with the lightweight characteristics and the ability to resist many common attacks simultaneously is proposed in this paper, at the same time the security route selection algorithm is also optimized by taking trust degree and QoS metrics into account. Performance analysis and simulation results show that TSSRM can improve the security and effectiveness of WSN.

Indexed Terms- Trust Management, Routing, Wireless Sensor Network, Data Transmission, Energy Consumption

I. INTRODUCTION

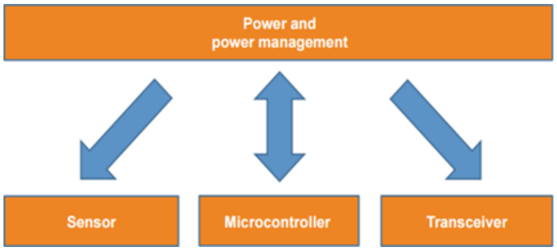
A WSN can generally be described as a network of nodes that cooperatively sense and control the environment, enabling interaction between persons or computers and the surrounding environment. WSNs nowadays usually include sensor nodes, actuator nodes, gateways and clients. A large number of sensor nodes deployed randomly inside of or near the monitoring area (sensor field), form networks through self-organization. Sensor nodes monitor the collected data to transmit along to other sensor nodes by hopping. During the process of transmission, monitored data may be handled by multiple nodes to get to gateway node after multihop routing, and finally reach the management node through the internet or satellite. It is the user who configures and manages the WSN with the management node; publish monitoring missions and collection of the monitored data.

As related technologies mature, the cost of WSN equipment has dropped dramatically, and commercial fields. Meanwhile, standards for WSN technology have been well developed, such as Zigbee, Wireless Hart, ISA 100.11a, wireless network for industrial automation- process automation,etc.

Moreover, with new application modes of WSN emerging in industrial automation and home applications, the total market size of WSN application will continue to growrapidly.

II. SENSOR NODES

The sensor node is one of the main parts of a WSN. The hardware of a sensor node generally. Include four parts: the power and power management module, a sensor, a microcontroller, and a wireless transceiver.



The power module offers the reliable power needed for the system. The sensor is the bond of WSN node which can obtain the environmental and equipment status. A sensor is in charge of collecting and transforming the signals, such as light, vibration and chemical signals, into electrical signals and then transferring them to the microcontroller. The microcontroller receives the data from the sensor and processes the data accordingly. The Wireless Transceiver(RF module) then transfer the data, so that the physical realization of communication can be achieved. It is important than the design of the all parts of a WSN node consider the WSN node features of tiny size and limitedpower.

III. TOPOLOGY

Generally, a WSN consists of a number of sensor network nodes and a gateway for theconnection to the internet. First, the sensor network nodes broadcast their status to the surroundings and receive status from other nodes to detect each other.

Second, the sensor network nodes are organized into a connected network according to a certain topology (linear, star, tree, mesh, etc.). Finally, suitable paths are computed on the constructed network for transmitting the sensing data.

IV. DATA AGGREGATION

Data aggregation is the process of integrating multiple copies of information into one copy, which is effective and able to meet user needs in middle sensor nodes. The introduction of data aggregation benefits both from saving energy and obtaining accurate information. The energy consumed in transmitting data is much greater than that in processing data in sensor networks. Therefore, with the node’s local computing and storage capacity, data aggregating operations are made to remove large quantities of redundant information, so as to minimize the amount of transmission and save energy.

In the complex network environment, it is difficult to ensure the accuracy of the information obtained only by collecting few samples of data from the distributed sensor nodes. As a result, monitoring the data of the same object requires the collaborative work of multiple sensors which effectively improves the accuracy and the reliability of the information obtained

V. SECURITY

The question of individual privacy and security within this for the individual becomes more difficult as the complex chain within which the security has been created is infinite and the weakest link defines the overall level of security.

The question is whether they can all be secured to a level that can ensure individual privacy rights and secure the systems from malicious attacks. In traditional TCP/IP networks, security is built to protect the confidentiality, integrity and availability of network data. It makes the system reliable and protects the system from malicious attacks which can lead to malfunctioning systems and information disclosure. As the characteristic of node and application environment, WSN security not only needs traditional security protection, but also the special requirements of trust, security and privacy (TSP)WSNs.

VI. RELATED WORK

Many research works have investigated the problem of malicious node detection. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative black hole attacks. In addition, some of these methods require specific environments or assumptions in order to operate. In general, detection mechanisms that have been proposed so far can be grouped into two broad categories. Proactive detection schemes are schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of the existence of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted.

However, one of the advantages of these types of schemes is that it can help in preventing or avoiding an attack in its initial stage. Reactive detection schemes [are those that trigger only when the destination node detects a significant drop in the packet delivery ratio. Among the above schemes are the ones proposed in and which we considered as benchmark schemes for performance comparison purposes. The scheme for the detection of routing misbehaviour. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received.

VII. EXISTING SYSTEM

Existing system is nothing but already have in our or doing project. In this session we discuss the construction of baseline models of existing systems. This project analyzes the behaviour of sensor nodes, including the movement and energy consumption of sensor nodes. The trust degree of sensor node is evaluated according to these characters, and then the trust degree of route is calculated and the trust calculation model of network is established to get the optimal route from the source node to the destination node.

VIII. DISADVANTAGES

In this session we discuss the construction of baseline models of existing systems. This project analyses the behaviour of sensor nodes, including the movement and energy consumption. It is an optimal route from the source node to the destination node.

IX. PROPOSED SYSTEM

Proposed system means you modified the particular pattern of doing paper is called "proposed system". In proposed system, we overcome the drawback of existing system. To overcome the issues we propose a security and trust routing through an active detection route protocol is proposed in this paper. The Active Trust scheme is the first routing scheme that uses active detection routing to address BLA. The Active Trust route protocol has better energy efficiency. The Active Trust scheme has better security performance. The Active Trust routing scheme proposed in this paper can improve the success routing probability by 1.5 times to 6 times and the energy efficiency by more than 2 times compared with that of previous researches. An overview of the Active Trust scheme, which is composed of an activedetection routing protocol and data routing protocol.

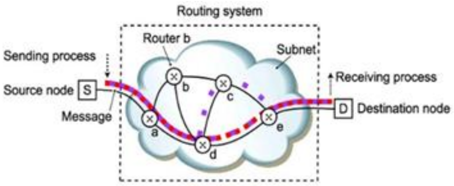
The Active Trust scheme has better security performance. Compared with previous research, nodal trust can be obtained in Active Trust. The route is created by the following principle. First, choose nodes with high trust to avoid potential attack, and then route along a successful detection route. Through the above approach, the network security can be improved.

Through our extensive theoretical analysis and simulation study, the Active Trust routing scheme proposed in this paper can improve the success routing probability by 1.5 times to 6 times and the energy efficiency by more than 2 times compared with that of previous researches.

X. SPECIFIC FEATURES

- The active trust scheme is the first routing scheme.
- That uses active detection routing to address BLA.
- Active trust route protocol has better energy efficiency.
- The active trust scheme has better security performance.
- The active trust routing scheme proposed in this paper can improve the success routing probability.

XI. SYSTEM MODEL



Routing system

Wireless Sensor Networks (WSNs) are emerging as a promising technology because of their wide range of applications in industrial, environmental monitoring, military and civilian domains. Due to economic considerations, the nodes are usually simple and low cost. They are often unattended, however, and are hence likely to suffer from different types of novel attacks. A black hole attack (BLA) is one of the most typical attacks and works as follows.

The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to be forwarded to the sink. Because the network makes decisions depending on the nodes' sensed data, the consequence is that the network will completely fail and, more seriously, make incorrect decisions. Therefore, how to detect and avoid BLA is of great significance for security inWSNs.

However, the current trust-based route strategies face some challenging issues. The core of a trust route lies in obtaining trust. However, obtaining the trust of a node is very difficult, and how it can be done is still unclear and Energy efficiency. Because energy is very limited in WSNs, in most research, the trust acquisition and diffusion have high energy consumption, which seriously affects the network lifetime and Security. Because it is difficult to locate malicious nodes, the security route is still a challenging issue. Thus, there are still issues worthy of further study. Security and trust routing through an active detection route protocol is proposed in this paper. The main innovations are as follows.

The Active Trust scheme is the first routing scheme that uses active detection routing to address BLA. The most significant difference between Active Trust and previous research is that we create multiple detection routes in regions with residue energy; because the attacker is not aware of detection routes, it will attack these routes and, in so doing, be exposed. In this way, the attacker’s behaviour and location, as well as nodal trust, can be obtained andused to avoid black holes when processing real data routes. To the best of our knowledge, this is the first proposed active detection mechanism in WSNs.

XII. METHODOLOGY

A hash function takes a variable length message and produces a fixed length message as its output. This output message is called the hash or message digest of the original input message. The trick behind building a good, secured cryptographic hash function is to devise a good compression function in which each input bit affects as many output bits as possible. The SHA-1 algorithm belongs to a set of cryptographic hash functions similar to the MD family of hash functions. But the main difference between the SHA-1 and the MD family is the more frequent use of input bits during the course of the hash function in the SHA-1 algorithm than in MD4 or MD5. This fact results in SHA-1 being more secured compared to MD4 or MD5 but at the expense of slower execution. The original specification of the algorithm was published in May 1993 whereas the revised version was published in1995.

The algorithm was based on principles similar to those in the design of the MD4 and MD5 algorithms .The way this algorithm works is that for a message of size < 264 bits it computes a 160-bit condensed output called a message digest. The SHA-1 algorithm is designed so that it is practically infeasible to find two input messages that hash to the same output message. It is also practically impossible to deduce the original input message given only the output hash message as stated before the SHA-1 algorithm produces a condensed representation of the given input message or data file. This input message is considered as a bit string where the length of the message is the number of bits in the input string. The purpose of message padding is to produce a padded message of length equal to a multiple of 512 bits. The reason behind this is that the SHA-1 algorithm processes messages as ‘n’ number of 512-bit blocks when computing the message digest.

SHA-1 is one of the required secure hash algorithms for use in U.S. Federal applications for the motive of protecting highly sensitive data of the most important applications of the SHA-1 algorithm is its incorporation in the Digital Signature Standard. It is used commonly with the Digital Signature Algorithm in electronic mail, electronic funds transfer, software distribution and various other applications that demand data integrity and authentication. The idea of signing hashed messages provides many advantages, one of them being faster creation and less resourcesfor storage or transmission .Few other applications include the SHACAL block ciphers, copy prevention system of Microsoft’s Xbox game console and many file sharing applications.

XIII. CONCLUSION

In this paper, we have proposed a novel security and trust routing scheme based on active detection, and it has the following excellent properties: (1) High successful routing probability, security and scalability. The Active Trust scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly 100% successful routing probability. (2) High energy efficiency. The Active Trust scheme fully uses residue energy to construct multiple detection routes. The theoretical analysis and experimental results have shown that our scheme improves the successful routing probability by more than 3 times, up to 10 times in some cases. Further, our scheme improves both the energy efficiency and the network security performance. It has important significance for wireless sensor networksecurity.

Cloud computing has been attracting the attention of several researchers both in the academia and the industry as it provides many opportunities for organizations by its powerful data storage and data processing abilities. In our future, we can integrate Mobile Adhoc Networks (MANETs) with cloud computing to enable convenient, on-demand network access for a shared pool of configurable computing resources.

XIV. FUTURE SCOPE

The further progress is based on the simulation of the appropriate programmer. For that the analysis of Simulator is mandatory. The analysis includes the scope as well as criticisms of simulator which will be followed by tracing. NS programming is the next step which required for the simulation which leads to a study on creation topology helpful for tracing and animation. After that the data transmission and its related observations have to be done. By means of that the packet loss and other errors have to be verified and thus hopefully the topic will reach the assumed conclusion with final output. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewingfacilities.

REFERENCES

[1] J. G. Choi, S. Bahk, ”Cell-throughput analysis of the proportional fair scheduler in the single-cell environment,” IEEE Transactions on Vehicular Technology, vol. 56, no. 2, pp. 766-778,2007.

[2] J. M. Chang, T. Po-Chun, W. G. Isaac, C. C. Han, and C. F. Lai, ”Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach,” IEEE Systems Journal, vol. 9, no. 6, pp. 65-75,2015.

[3] Dr.R.Vijayarajeswari, A Rajivkannan,”Survey of Malicious Node Detection in Wireless Sensor Networks,” Asian Journal of Research in Social Sciences and Humanities 7 (2), 624-631, 2017.

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang,andW. Zhao, ”A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet of Things Journal, vol. PP, no. 99, pp. 1-18, 2017.

[5] R. Morsi, DS. Michalopoulos, and R. Schober, ”Multiuser scheduling schemes for simultaneous wireless information and power transfer over fading channels,” IEEE Transactions on Wireless Communications, vol. 14, no. 4, pp. 1950-1964, 2015.

[6] O. Ozel, K. Tutuncuoglu, J. Yang, S. Ulukus,andA. Yener, ”Transmission with energy harvesting nodes in fading wireless channels: optimal policies,” IEEE Journal on Selected Areas in Communications, vol. 29, no. 8, pp. 1732-1743, Sep. 2011.

[7] Dr.R.Vijayarajeswari,J.Santhosh” An Effective Apporach for Malicious Node Detection in Wireless Sensor Networks using Classifier,”Asian Journal of Research in Social Sciences and Humanities 6 (11), 81-91,2017

[8] G. Ottman, A. Bhatt, H. Hofmann, and G. Lesieutre, ”Adaptive piezoelectric energy harvesting circuit for wireless, remote power supply,” IEEE Transactions on Power Electronics, vol. 17, no. 5, pp. 669-676, Sep.2002.

[9] A. K. A. Mohammad, and S. Gadadhar, ”Enhancing cooperation in MANET using neighborhood compressive sensing model,” Egyptian Informatics Journal, vol. 6, no. 1, pp. 1-15,2016.

[10] P. Balasubramanian, J. V. P. Maria, K. Madasamy, ”Development of a secure routing protocol using game theory model in mobile ad hoc networks,” Journal of Communications and Networks, vol. 17, no. 13, pp. 75-83,2015.

[11] I. Krikidis, S. Timotheou, S. Nikolaou, and G. Zheng, ”Simultaneous wireless information and

power transfer in modern communication systems,” IEEE Communications Magazine, vol. 52, no. 11, pp. 16424- 16450,2014.

[12] G. Uttam G, and D. Raja,”SDRP: secure and dynamic routing protocol for mobile ad-hoc networks,” IET Networks, vol. 3, no. 2, pp. 235-243, 2014.

[13] X. Du, and H. Chen, ”Security in Wireless Sensor Networks,” IEEE Wireless Communications, vol. 15, no. 4, pp. 60-66,2008.

[14] N. Marlon, C. Jose, A. B. Campelo, O.Rafael,V. C. Juan, and J. S. Juan, ”Active low intrusion hybrid monitor for wireless sensor networks,” Sensors, vol. 15, no. 3, pp. 23927-23952, 2015.

[15] Dr.R.Vijayarajeswari,J. Santhosh "Performance Analysis of Residual Node Detection and Mitigation Using Feature Set and Classification Approach", International Journal of Printing, Packaging &Allied Sciences 4 (4),2856-2863,2016