RESEARCH ON TRUST SENSING BASED SECURE ROUTING MECHANISM FOR WIRELESS SENSOR NETWORK

Janani . P[1] C.Renuga[2] C.Tamilselvi[3]
Bharathiyar Arts And Science College For Women, Deviyakurichi

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.

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 their applications are gradually expanding from the military areas to industrial and commercial fields. Meanwhile, standards for WSN technology have been well developed, such as Zigbee, Wireless Hart, ISA 100.11a, wireless networks for industrial automation – process automation (WIA-PA), etc. Moreover, with new application modes of WSN emerging in industrial automation and home applications, the total market size of WSN applications will continue to grow rapidly.

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 blackhole 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 misbehavior. 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.

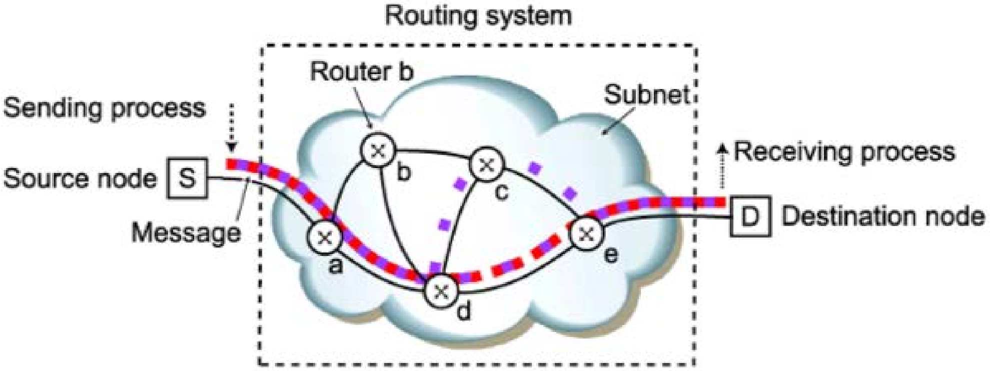
PROPOSED SYSTEM

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 active detection routing protocol and data routing protocol.

ADVANTAGES:

- 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 .

SYSTEM MODEL:



Existing routing system

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 network security.

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.

REFERENCE

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

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. 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, and A. 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] 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.

[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.