Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X

Vol.3 Issue 4 (2017) 16 - 22. Submitted 01/11/2017. Published 10/12/2017

SECURE ROUTING IN WIRELESS SENSOR NETWORKS

[1]K.Gayathri, M.Phil Scholar, Department Of Computer Science, Shri Sakthikailassh Women's College, Salem,

[2]J.Shanbagam, Assistant Professor, Department Of Computer Science, Shri Sakthikailassh Women's College, Salem.

ABSTRACT

Wireless Sensor Networks (WSNs) are unindustrialized as an propitious technology for the reason that of their wide mixture of presentations in industrial, eco-friendly specialist care, etc. For the reason that of their inherent resource-constrained characteristics, they are prone to various security attacks, in addition to a black hole attack is a type of attack that extremely distresses statistics assemblage. The contemporary trust-based route strategies appearance some challenging issues: the core of a trust route lies in earning trust. Energy efficiency. Currently, WSN (Wireless Sensor Network) is the most standard services employed in commercial and industrial applications, because of its technical development in a processor, communication, and low-power usage of embedded computing devices. The WSN is built with nodes that are used to observe the surroundings like temperature, humidity, pressure, position, vibration, sound etc. These nodes can be used in various real-time applications to perform various tasks like smart detecting, a discovery of neighbor node, data processing and storage, data collection, target tracking, monitor and controlling, synchronization, node localization, and effective routing between the base station and nodes.

Keywords: WSN, Data processing, Data collection.

1. 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. The sensor node is a multi-functional, energy efficient wireless device. The applications of motes in industrial are widespread. A collection of sensor nodes collects the data from the surroundings to achieve specific application objectives. The communication between motes can be done with each other using transceivers. In a wireless sensor network, the number of motes can be in the order of hundreds/ even thousands. In contrast with sensor n/ws, Ad Hoc networks will have fewer nodes without any structure. The function of the transport layer is to deliver congestion avoidance and reliability where a lot of protocols intended to offer this function are either practical on the upstream. These protocols use dissimilar mechanisms for loss recognition and loss recovery. The transport layer is exactly needed when a system is planned to contact other networks. 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.

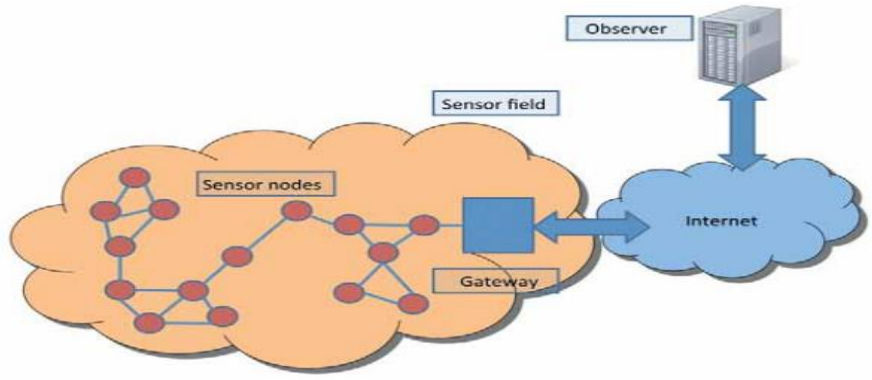

Fig 1.1: Wireless sensor networks

2. RELATED WORK

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 ActiveTrust scheme is the first routing scheme that uses active detection routing to address BLA. The most significant difference between ActiveTrust 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 behavior and location, as well as nodal trust, can be obtained and used 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.

The ActiveTrust route protocol has better energy efficiency. Energy is very precious in WSNs, and there will be more energy consumption if active detection is processed. Therefore, in previous research, it was impossible to imagine adopting such high-energy-consumption active detection routes. However, we find it possible after carefully analyzing the energy consumption in WSNs. Research has noted that there is still up to 90% residue energy in WSNs when the network has died due to the "energy hole" phenomenon.

3. 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 activity relies on knowledge of the hardware, software, workload, and monitoring tools associated with the system under study.

The nodes in wireless sensor networks are suffered from different types of novel attacks. A black hole attack (BLA) is one of the most typical attacks. There is much research on black hole attacks. Such studies mainly focus on the strategy of avoiding black holes. Another approach does not require black hole information in advance. In this approach, the packet is divided into M shares, which are sent to the sink via different routes (multi-path), but the packet can be resumed with T shares (T<=M).

However, a deficiency is that the sink may receive more than the required T shares, thus leading to high energy consumption.

Another preferred strategy that can improve route success probability is the trust route strategy. The main feature is to create a route by selecting nodes with high trust because such nodes have a higher probability of routing successfully; thus, routes created in this manner can forward data to the sink with a higher success probability. However, the current trust-based route strategies face some challenging issues.

The fig 3.1 depicted below helps us to gain a thorough knowledge on our existing work. This workflow describes the sequence in which the existing system works. Finally we also discuss the metrics that is being used in the existing system.

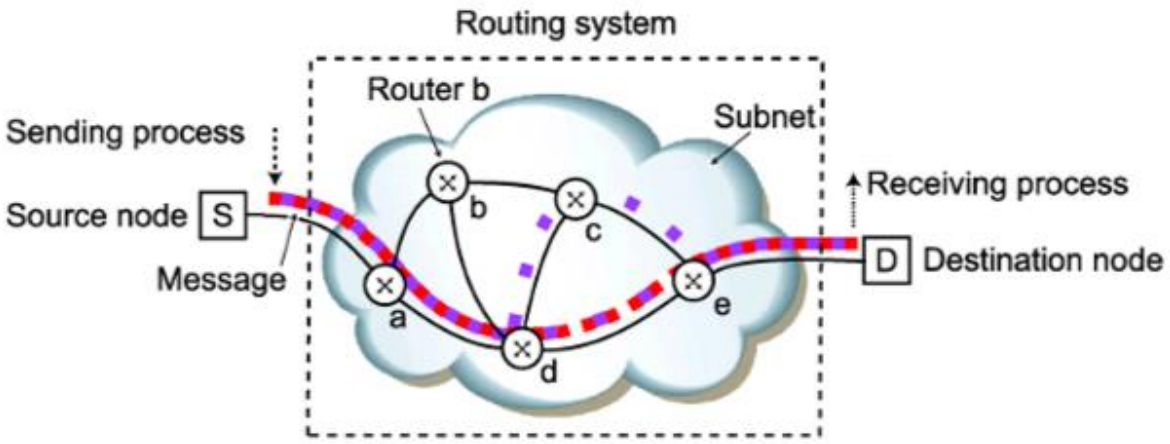

Fig 3.1: Existing routing system

Some of the limitations of the existing system are,

(1) 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.
(2) 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.
(3) Security. Because it is difficult to locate malicious nodes, the security route is still a challenging issue.

4. PROPOSED SYSTEM

Proposed system means you modified the particular pattern of doing project 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 project. The main innovations are as follows.

- ✓ The ActiveTrust scheme is the first routing scheme that uses active detection routing to address BLA.
- ✓ The ActiveTrust route protocol has better energy efficiency.
- ✓ The ActiveTrust scheme has better security performance.
- ✓ The ActiveTrust routing scheme proposed in this project 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 ActiveTrust scheme, which is composed of an active detection routing protocol and data routing protocol, is shown in Fig. 3.2

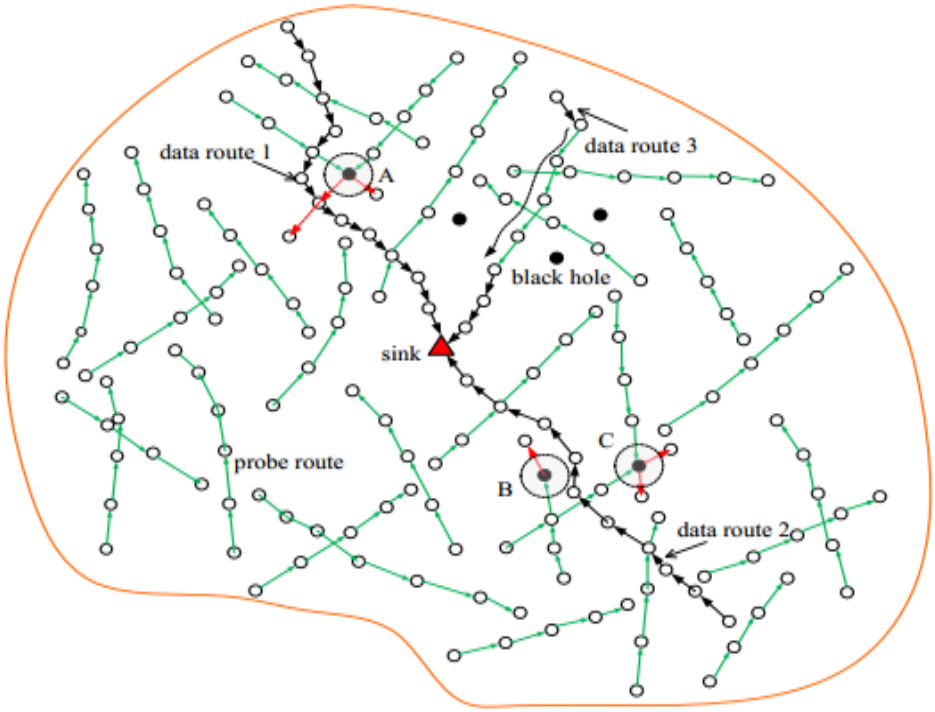

Fig 3.2:Illustration of the ActiveTrust scheme

Active Detection Routing Protocol: A detection route refers to a route without data packets whose goal is to convince the adversary to launch an attack so the system can identify the attack behaviour and then mark the black hole location. Thus, the system can lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Wireless sensor networks may comprise of numerous different types of sensors like low sampling rate, seismic, magnetic, thermal, visual, infrared, radar, and acoustic, which are clever to monitor a wide range of ambient situations. Sensor nodes are used for constant sensing, event ID, event detection & local control of actuators. The applications of wireless sensor network mainly include health, military, environmental, home, & other commercial areas.

5. MODULES

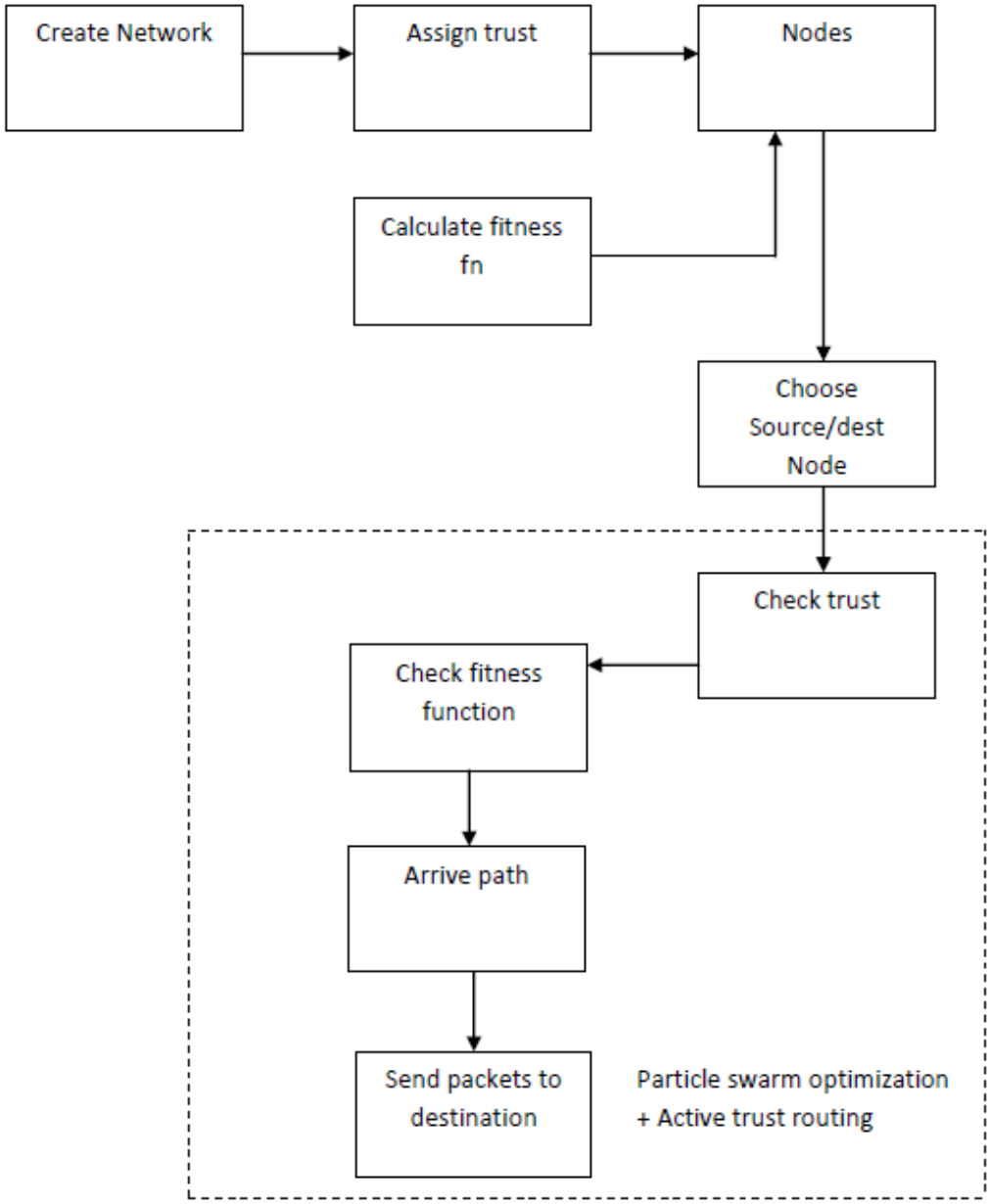

Figure: Architecture Diagram for Proposed System

Active detection routing

A detection route refers to a route without data packets whose goal is to convince the adversary to launch an attack so the system can identify the attack behaviour and then mark the black hole location. Thus, the system can lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Through active detection routing, nodal trust can be quickly obtained, and it can effectively guide the data route in choosing nodes with high trust to avoid black holes.

Data routing

The data routing refers to the process of nodal data routing to the sink. The routing protocol is similar to common routing protocols in WSNs [3, 7, 8]; the difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink. The data routing is shown via the black arrow in . The routing protocol can adopt an existing routing protocol [7, 12], and we take the shortest route protocol as an example

Packet Transfer

The topology of the swarm defines the subset of particles which each particle can exchange information. The basic version of the algorithm uses the global topology as the swarm communication structure. This topology allows all particles to communicate with all the other particles, thus the whole swarm share the same best position g from a single particle. However, this approach might lead the swarm to be trapped into a local minimum, thus different topologies have been used to control the flow of information among particles. For instance, in local topologies, particles only share information with a subset of particles. This subset can be a geometrical one – for example "the m nearest particles" – or, more often, a social one, i.e. a set of particles that is not depending on any distance. In such a case, the PSO variant is said to be local best (vs global best for the basic PSO).

Network model security

A commonly used swarm topology is the ring, in which each particle has just two neighbours, but there are many others. The topology is not necessarily static. In fact, since the topology is related to the diversity of communication of the particles, some efforts have been done to create adaptive topologies (SPSO, stochastic star, TRIBES, Cyber Swarm, and C-PSO).

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 ActiveTrust 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 ActiveTrust 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.

BIBLIOGRAPHY

1. Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency,"IEEE System Journal, Doi: 10.1109/JSYST.2014.2308391, 2014.

2. M. Dong, K. Ota, A. Liu, et al. "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks," IEEETransactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 225-236, 2016.

3. S. He, J. Chen, F. Jiang, et al. "Energy provisioning in wireless rechargeable sensor networks," IEEE transactions on mobile computing, vol. 12, no. 10, pp. 1931-1942, 2013.

4. X.Liu,M. Dong, K. Ota, P. Hung, A. Liu. "Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory," IEEE Transactions on Services Computing,vol. 9, no. 2, pp. 186-198, 2016.

5. C. Zhu, H. Nicanfar, V. C. M. Leung, et al. "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2015.

6. A.Liu, M.Dong, K.Ota, et al."PHACK : An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs," Sensors, vol. 15, no. 12, pp. 30942-30963, 2015.

7. A. Liu, X. Jin, G.Cui, Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network,"InformationSciences,vol. 230, pp.197-226, 2013.

8. Z. Zheng, A. Liu, L. Cai, et al."Energy and Memory Efficient Clone Detection in Wireless Sensor Networks,"IEEE Transactions on Mobile Computing.vol. 15, no. 5, pp.1130-1143,2016.