SUKANYA G, et al, International Journal of Computers, Electrical and Advanced Communication Engineering [IJCEACE]™. Thomson Reuters Research ID: D-1150-2018, Volume 1, Issue 15, PP: 22 - 26, JAN - JUL' 2019.

ACTIVETRUST: SECURE AND TRUSTABLE ROUTING IN WIRELESS SENSOR NETWORKS

G SUKANYA 1*, B PRUDHVI 2*

1. *II.M.Tech , Dept of CSE, MOTHER TERESA INSTITUTE OF SCIENCE AND TECHNOLOGY.*
2. *Asst. Prof, Dept. of CSE, MOTHER TERESA INSTITUTE OF SCIENCE AND TECHNOLOGY.*

ABSTRACT — Wireless sensor networks (WSNs) are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. To conquer that challenge, an active detection-based security and trust routing scheme named ActiveTrust is proposed for WSNs. The most important innovation of ActiveTrust is that it avoids black holes through the active creation of a number of detection routes to quickly detect and obtain nodal trust and thus improve the data route security. More importantly, the generation and distribution of detection routes are given in the ActiveTrust scheme, which can fully use the energy in non-hotspots to create as many detection routes as needed to achieve the desired security and energy efficiency. Both comprehensive theoretical analysis and experimental results indicate that the performance of the ActiveTrust scheme is better than that of previous studies. ActiveTrust can significantly improve the data route success probability and ability against black hole attacks and can optimize network lifetime.

INTRODUCTION

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 [1-5]. 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 [6-8]. A black hole attack (BLA) is one of the most typical attacks [9] 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 [10-15]. Therefore, how to detect and avoid BLA is of great significance for security in WSNs.

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 [10-15]. Therefore, how to detect and avoid BLA is of great significance for security in WSNs.

EXISTING SYSTEM

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 in WSNs. There is much research on black hole attacks. However, the current trust-based route strategies face some challenging issues. (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.

Disadvantages of Existing System:

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.

PROPOSED SYSTEM

In this paper we propose security and trust routing through an active detection route *protocol.* 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.

Advantages of Proposed System:

The ActiveTrust scheme is the first routing scheme that uses active detection routing to address Blockhole attacks (BLA)

The ActiveTrust route protocol has better energy efficiency

The ActiveTrust scheme has better security performance

SYSTEM ARCHITECTURE

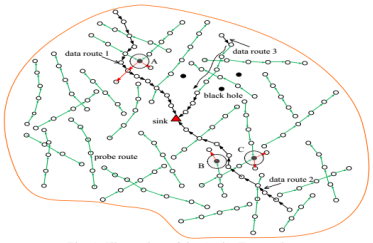

Fig. 1: Illustration of the ActiveTrust scheme

MODULES

We have two modules,

1. Detection Route Module
2. Data Routing Module

Module Description:

Detection Route:

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 behavior and then mark the black hole location.

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; 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.

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

REFERENCES

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," IEEE Transactions 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," Information Sciences, 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. 9. T. Shu, M. Krunz, S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941-954, 2010. 10. P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog

Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015