International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 04 | April-2021 ISSN: 2582-3930

Fast Detection of Transformed Data Leaks in Wireless Sensor Network

SATHISH KUMAR K[1], THANGAM M[2], SOWMIYA M[3]

[1]*Computer Science and Engineering &M.A.M. School of Engineering, Trichy*
[2]*Computer Science and Engineering & M.A.M. School of Engineering, Trichy*
[3]*Computer Science and Engineering & M.A.M. School of Engineering, Trichy*

Abstract -Wireless Sensor Networks (WSNs) are emerging as a promising technology because of their wide range of applications in industrial, environmental monitoring, etc. Because of their inherent resource-constrained characteristics, they are prone to various security attacks that seriously affect data collection.The current trust-based route strategies face some challenging issues: (1) the core of a trust route lies in obtaining trust. (2) Energy efficiency. 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 project. The Active Trust scheme fully uses residue energy to construct multiple detection routes.

Key Words:resource-constrained, trust-based, Energy efficiency

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 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. It is the user who configures and manages the WSN with the management node: publishes monitoring missions and collection of the monitored data.

2. OBJECTIVE

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 the potential attack, and then route along a successful detection route. Through the above approach, network security can be improved.

3. EXISTING SYSTEM

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.

4. DISADVANTAGES

Attacks in mobile wireless networks are very challenging because the network topology can be highly dynamic due to node movements. Therefore, techniques that are designed for static networks are not applicable.

The network may not always be connected. Therefore, approaches that rely on network connectivity have limited applicability.

The limited resources (computation, communication, and battery life) demand that node attacks must be performed in a resource-conserving manner.

5. LITERATURE SURVEY

AD HOC ON-DEMAND DISTANCE VECTOR ROUTING:

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology timely manner. The operation of AODV is loop-free, and avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they can invalidate the routes using the lost link.

GRADIENT-BASED ROUTING:

The key idea in GBR is to memorize the number of hops when the interest is diffused through the whole network. As such, each node can calculate a parameter called the height of the node, which is the minimum

number of hops to reach the BS. The difference between a node's height and that of its neighbor is considered the gradient on that link. A packet is forwarded on a link with the largest gradient. GBR uses some auxiliary techniques such as data aggregation and traffic spreading to uniformly divide the traffic over the network. When multiple paths pass through a node, which acts as a relay node, that relay node may combine data 12 according to a certain function.

6. ROUTING PROTOCOLS WITH RANDOM WALKS

The objective of the random walks-based routing technique is to achieve load balancing in a statistical sense and by making use of multi-path routing in WSNs. This technique considers only large-scale networks where nodes have very limited mobility. In this protocol, it is assumed that sensor nodes can be turned on or off at random times. Further, each node has a unique identifier but no location information is needed. Nodes were arranged such that each node falls exactly on one crossing point of a regular grid on a plane, but the topology can be irregular.

7. PROPOSED SYSTEM

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 behavior and then mark the attack 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 attacks.

8. ADVANTAGES

Our approach has the advantage that it is applicable to both connected and disconnected networks.
Our schemes achieve high failure detection rates, low false-positive rates, and low communication overhead.

Table -1: Software & Hardware Requirements

Software Specification

Server Side Programming	PHP.
Middleware Programming	JAVASCRIPT
Operating System	Windows 8
Web Server	Internet Information Server
Client Script	HTML, CSS and Java Script
Database	MYSQL

Hardware Specification

Processor	Intel Core i3-2330M CPU 2.20 GHz
Hard Disk	160 GB
Monitor	LG 17" Color Monitor
RAM	4 GB
Keyboard	104 Keys Multimedia Keyboard
Mouse	wireless Optical Mouse
CD – ROM	52X CD-ROM

9. SYSTEM ARCHITECTURE

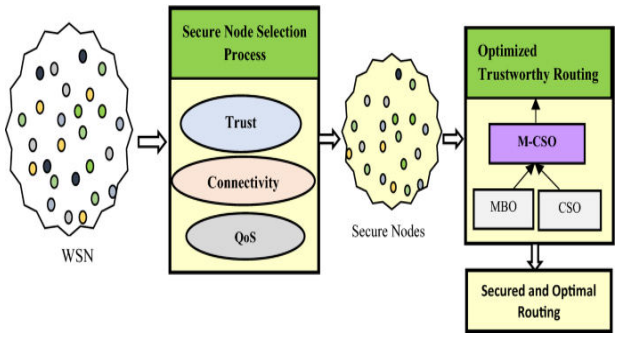

Fig -1: Figure

3. CONCLUSIONS

The 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 energy efficiency and 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.