A NOVEL APPROACH FOR SECURITY AND TRUST ROUTING
SCHEME IN WSN BASED ON ACTIVE DETECTION

1MS, R.RUBI PARKAVI, M.E., 2Mr. T.PERIYASAMY, M.E.,
1PG SCHOLAR DEPARTMENT OF COMPUTER SCIENCE ENGINEERING1,
2ASSISTANT PROFESSOR DEPARTMENT OF COMPUTER SCIENCE ENGINEERING2,
MRK INSTITUTE OF TECHNOLOGY,
KATTUMANNARKOIL, INDIA,
pdharshni66@gmail.com, periyasamy2204@gmail.com

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, and a black hole attack is a type of attack that seriously affects 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 ActiveTrust scheme fully uses residue energy to construct multiple detection routes. The theoretical analysis and experimental results have shown that our scheme improves successful routing probability by more than 3 times, up to 10 times in some cases.

Index Term: Resource constrained, Route strategies, malicious nodes, ActiveTrust.

I. 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. 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 in wireless sensor networks (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. Therefore, the ActiveTrust scheme takes full advantage of the residue energy to create detection routes and attempts to decrease energy consumption in hotspots (to improve network lifetime). Those detection routes can detect the nodal trust without decreasing lifetime and thus improve the network security. According to theoretical analysis and experimental results, the energy efficiency of the ActiveTrust scheme is improved more than 2 times compared to previous routing schemes, including Through our extensive theoretical analysis and simulation study, the ActiveTrust 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.

II. RELATED WORK

Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency" How to sense and monitor the environment with high quality is an important research subject in the Internet of Things (IOT). This paper deals with the important issue of the balance between the quality of target detection and lifetime in wireless sensor networks. Two target-monitoring schemes are proposed. One scheme is Target Detection with Sensing Frequency K (TDSFK), which distributes the sensing time that currently is only on a portion of the sensing period into the entire sensing period. That is, the sensing frequency increases from 1 to K. The other scheme is Target Detection with Adjustable Sensing Frequency (TDASF), which adjusts the sensing frequency on those nodes that have residual energy. The simulation results show that the TDASF scheme can improve the network lifetime by more than 17.4% and can reduce the weighted detection delay by more than 101.6%.
A. Liu, M. Dong, K. Ota, et al. "PHACK: An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs", in this paper, a Per-Hop Acknowledgement (PHACK)-based scheme is proposed for each packet transmission to detect selective forwarding attacks. In our scheme, the sink and each node along the forwarding path generate an acknowledgement (ACK) message for each received packet to confirm the normal packet transmission. The scheme, in which each ACK is returned to the source node along a different routing path, can significantly increase the resilience against attacks because it prevents an attacker from compromising nodes in the return routing path, which can otherwise interrupt the return of nodes' ACK packets. For this case, the PHACK scheme also has better potential to detect abnormal packet loss and identify suspect nodes as well as better resilience against attacks. Another pivotal issue is the network lifetime of the PHACK scheme, as it generates more acknowledgements than previous ACK-based schemes. We demonstrate that the network lifetime of the PHACK scheme is not lower than that of other ACK-based schemes because the scheme just increases the energy consumption in non-hotspot areas and does not increase the energy consumption in hotspot areas. Moreover, the PHACK scheme greatly simplifies the protocol and is easy to implement. Both theoretical and simulation results are given to demonstrate the effectiveness of the proposed scheme in terms of high detection probability and the ability to identify suspect nodes.

A. Liu, X. Jin, G. Cui, Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network", The demand for maximum network lifetime in many mission-critical applications of wireless sensor networks motivates the great significance to deploy as few sensors as possible to achieve the expected network performance. In this paper, we first characterize the energy consumption of wireless sensor networks with adjustable transmission ranges through theoretical analysis. Based on this result, we propose a deployment strategy with $T$ as the required minimum network lifetime. We come up with three interventions: (A) in order to achieve an evenly balanced energy consumption among all nodes, the node density in different areas of the network should be a continuous varying function of...
the distance from the sink; (B) if there are insufficient nodes to achieve a balanced energy consumption over the whole network, our proposed node deployment strategy can be used to achieve the required lifetime threshold $T$ with minimum number of nodes; and (C) when there are sufficient nodes to ensure the network connectivity and coverage with the node density of $\tau$, we design an algorithm to identify the optimal transmission radius $r$ and the corresponding achievable maximum network lifetime. Our conclusions are verified by extensive simulation results.

T. Shu, M. Krunz, S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes", Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs). In this paper, we study routing mechanisms that circumvent (bypass) black holes formed by these attacks. We argue that existing multi-path routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes. In this paper, we develop mechanisms that generate randomized multipath routes. Under our design, the routes taken by the “shares” of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the routes generated by our mechanisms

III. SYSTEM ANALYSIS

Systems analysis is a problem solving technique that decomposes a system into its component pieces for the purpose of the studying how well those component parts work and interact to accomplish their purpose.

A. EXISTING WORK

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 ($T \leq M$). 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.

**B. LIMITATIONS**

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.

**C. PROPOSED WORK**

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.

**D. ADVANTAGES**

- 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
IV. SYSTEM DESIGN

System architecture is a conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

V. PARTICLE SWARM OPTIMIZATION

The individuals, called particles henceforth, are flown through the multidimensional search space with each particle representing a possible solution to the multi-dimensional optimization problem. Each solution's fitness is based on a performance function related to the optimization problem being solved. The movement of the particles is influenced by two factors using information from iteration-to-iteration as well as particle-to-particle. As a result of iteration-to-iteration information, the particle stores in its memory the best solution visited so far, called pbest, and experiences an attraction towards this solution as it traverses through the solution.
A. ALGORITHM

A basic variant of the PSO algorithm works by having a population (called a swarm) of candidate solutions (called particles). These particles are moved around in the search-space according to a few simple formulae. The movements of the particles are guided by their own best known position in the search-space as well as the entire swarm’s best known position. When improved positions are being discovered these will then come to guide the movements of the swarm. The process is repeated and by doing so it is hoped, but not guaranteed, that a satisfactory solution will eventually be discovered.

Formally, let \( f: \mathbb{R}^n \rightarrow \mathbb{R} \) be the cost function which must be minimized. The function takes a candidate solution as argument in the form of a vector of real numbers and produces a real number as output which indicates the objective function value of the given candidate solution. The gradient of \( f \) is not known. The goal is to find a solution \( a \) for which \( f(a) \leq f(b) \) for all \( b \) in the search-space, which would mean \( a \) is the global minimum. Maximization can be performed by considering the function \( h = -f \) instead.

\[
\text{for each particle } i=1, \ldots, s \text{ do}
\]

Initialize the particle’s position with a uniformly distributed random vector:

\[
x_i \sim \mathcal{U}(b_{lo}, b_{up})
\]

Initialize the particle’s best known position to its initial position: \( p_i \leftarrow x_i \)

\[\text{If } f(P_i) < f(g) \text{ then}\]

Update the swarm’s best known position: \( g \leftarrow p_i \)

Initialize the particle’s velocity:

\[
v_i \sim \mathcal{U}(-|b_{up}-b_{lo}|, |b_{up}-b_{lo}|)
\]

While a termination criterion is not met do:

\[
\text{for each particle } i=1,\ldots, s \text{ do}
\]
for each dimension \(d=1,\ldots, n\) do

Pick random numbers:
\[ r_p, r_g \sim u(0,1) \]

Update the particle’s velocity:
\[ v_{i,d} \leftarrow \alpha v_{i,d} + \Phi_p (p_{i,d} - x_{i,d}) + \Phi_g (g_d - x_{i,d}) \]

Update the particle’s position:
\[ x_i \leftarrow x_i + v_i \]

If \(f(x_i) < f(p_i)\) then

Update the particle’s best known position: \(p_i \leftarrow x_i\)

If \(f(p_i) < f(g)\) then

Update the swarm’s best known position: \(g \leftarrow p_i\)

VI. CONCLUSION

In this paper, 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.

REFERENCES


