TRUST BASED DETECTION OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORKS

Dilbag[1], Dinesh Kumar[2]

[1]*Research Scholar, Associate Professor, CSE Department*

Guru Gobind Singh College of Engineering and Technology, Guru Kashi University, Talwandi Sabo, Bathinda, India

Abstract: The unattended nature of wireless sensor networks (WSN) attracts many attackers to steal data from the network. Various attacks can be launched in such kind of network, out of which wormhole attack is one that focuses to tunnel creation to shorten the path length between two nodes. This paper proposes a modification to Energy-aware Secure Routing with Trust technique (ESRT) and computes the direct and indirect trust levels in a way that attack gets detected before its occurrence. The performance of the network was analyzed based on packet delivery ratio (PDR), throughput and remaining energy of the network. These parameters have shown an improvement over the existing scheme.

Keywords: Wireless sensor network, Trust model, direct trust, indirect trust, wormhole attack, PDR.

I. INTRODUCTION

Introduction of sensor nodes which are small, of low cost, and capable of sensing, communicating, and computing leads to the development of wireless sensor networks (WSNs) [1]. These nodes monitor the physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, or pollutants, at different locations. The monitored results are sent to base station, where all the data are collected and sent to user through Internet. A large number of nodes are deployed in open and harsh environments to obtain data from sensor field. Hence, this large number of nodes collaborates with each other to monitor the area and send the monitored result to base station. As capability of the node is limited in terms of sensing area and communication range, there is no choice but cooperating with other nodes in the network. Hence, cooperation of the nodes is vital for the performance of WSNs. Features of WSNs such as open and harsh environment, open medium, various important applications, and other factors make WSNs susceptible to different attacks [2].

Many solutions are introduced to secure WSNs, including routing. As routing performs data delivery to base station, it is vital protocol for WSNs. Hence, secure routing which is resilient against deliberate packet drops and alterations and disruption acts on routing operation is important. To secure routing, especially against compromised nodes, many solutions are proposed. One of such solutions is trust establishment [2, 3], used in many research fields [4, 5]. Trust establishment detects trustworthy and untrustworthy nodes by evaluating them on the basis of their past behavior/performance. It avoids untrustworthy nodes and selects only trustworthy in routing operation. Since trust mechanism is simple and efficient in compromised node detection, a significant research is done to enhance security and improve cooperation in the network.

This paper focuses on the wormhole attack in wireless sensor networks and Section II describes the existing techniques related to its detection and prevention. Section III presents the proposed modified trust aware routing schemes for its detection. Results have been described in Section IV and finally the paper has been concluded in the last section.

II. LITERATURE REVIEW

In this paper [6], the authors present an Energy-aware Secure Routing with Trust (ESRT) scheme that maintains a trusted environment and isolate misbehaving nodes. ESRT incorporates trust, energy, and hop counts for making routing decisions. This multifacet routing strategy helps to balance out energy consumption among trusted nodes while routing data using shorter paths. Simulation results demonstrate improved performance of the ESRT scheme when compared to existing work.

In this paper [7], the authors propose a security DV-Hop algorithm (AMLDV-Hop) to resist MWNL. Firstly, the algorithm establishes the Neighbor List (NL) in initialization phase. It uses the NL to find the suspect beacon nodes and then find the actually attacked beacon nodes by calculating the distances to other beacon nodes. The attacked beacon nodes generate and broadcast the conflict sets to distinguish the different wormhole areas. The unknown nodes take the marked beacon nodes as references and mark themselves with different numbers in the first-round marking. If the unknown nodes fail to mark themselves, they will take the marked unknown nodes as references to mark themselves in the second-round marking. The unknown nodes that still fail to be marked are semi-isolated. The results indicate that the localization error of proposed AMLDV-Hop algorithm has 112.3%, 10.2%, 41.7%, 6.9% reduction compared to the attacked DV-Hop algorithm, the Label-based DV-Hop (LBDV-Hop), the Secure Neighbor Discovery Based DV-Hop (NDDV-Hop), and the Against Wormhole DV-Hop (AWDV-Hop) algorithm.

The detection method in [8] is based on the concept of the rate of change of neighbouring nodes and the length of an alternative path between two nodes. The proposed method does not require any additional hardware such as synchronized clocks or timing information, GPS, or cryptographic methods that require large amounts of computational power. The simulation results indicate that our method has good detection accuracy.

The proposed method in [9] is used to analyze and detect the wormhole attack. Using EIGRP protocol to identify the shortest path and detect the attacking node based on the round trip time variation technique. As compared with previous method, it is the easy way to detect the wormhole attacks.

This paper [10] enhances security of Trust and energy aware secure routing protocol (TESRP) by securing it against wormhole attack. TESRP is one of the best trust based protocol but this protocol does not provide security from wormhole attack. In this paper trust algorithm together with sequence number concept has been used for securing TESRP from wormhole attack.

In this detection technique [11] it tries to prevent the attacks in LEACH protocol in a wireless sensor networks using the multiple base stations and key. Since, LEACH protocol is used, it guarantees power supply for a considerable amount of time with extra energy. This ensures that the packet delivery ratio has increased prolonging the lifetime of the network. The individual nodes are given more security, adding security to nodes will consume more energy thus reducing the lifetime of the network. If the nodes are solar aware, the energy level gets equalized and also surplus energy may be obtained because of usage of LEACH protocol. The proposed protocols are made to detect and prevent the attacks thus controlling the overhead, increasing packets delivered and extending the lifetime of the wireless sensor networks.

In this paper [12], a simple novel technique is proposed to detect the malicious wormhole node. The proposed methodology, to detect a wormhole considers the sudden change in traffic in each node as the metric. This is accomplished by setting counter values in sensor nodes. In this paper, wormhole attack is noticed by improving power consumption for each and every sensor node and it is well proven that power disbursed is less than other existing approaches. Main advantage is easy to find wormhole using simple methodology and external hardware is not necessary.

III. PROPOSED METHOD

The proposed model will use routing mechanism of AODV protocol. When a source node broadcasts a RREQ packet, every intermediate node broadcasts it until it reaches the destination node. During this broadcasting phase, the nodes can compute the direct trust using the formula given below. The nodes also forward their remaining energy level to their neighbors. If energy level is below a threshold value, RREQ packet is dropped otherwise it is forwarded to the next neighboring node.

The direct trust of the node is calculated as:

Direct trust = End to End delay * Hop count

For the tunnel based attacks, when nodes tunnel the route request packet to another pair, the end to end delay will be more and hop count will be less. This will reduce their direct trust. Indirect trust can be computed by averaging the direct trust of the common neighbors.

Indirect trust = Sum of Direct trust of common neighbors / number of common neighbors

When the route request reaches the destination node, it computes various paths to the source node. For all the paths, the destination computes the trust value. If for any node in any particular path, the trust value is found to be less than the threshold value than destination does not considers the nodes legitimate and marks them as malicious. For all the paths containing the legitimate nodes, the destination node also computes the composite routing function as

$$CRF = \alpha * T_{i,j}(t) + \beta * Energy \quad (1)$$

The weights α, β represent the significance of trust and energy respectively, where $\alpha+\beta=1$.

Destination node will send route reply to the source node over various paths. The source then makes final decision by choosing the route with most reliability, most remaining energy.

IV. RESULTS

The proposed scheme as well as the existing scheme [6] were implemented in network simulator 2.35. The network simulator is open source simulator and is operated in unix based environment. The network's performance was adjudged based on three parameters namely throughput, packet delivery ratio and remaining energy.

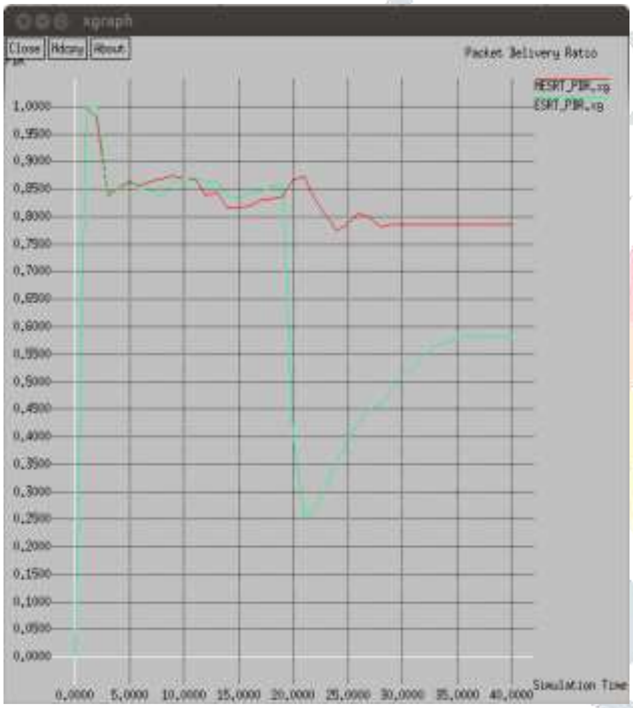

Figure 4.1: PDR Comparison

This graph shows the comparison of the packet delivery ratio for both the existing and modified schemes. The value of PDR for the existing scheme was found to be 58.23 percent and for the modified scheme, the value of PDR was 78.55 percent. For the existing scheme, the value of PDR shows a steep fall indicating the occurrence of attack before it gets detected eventually.

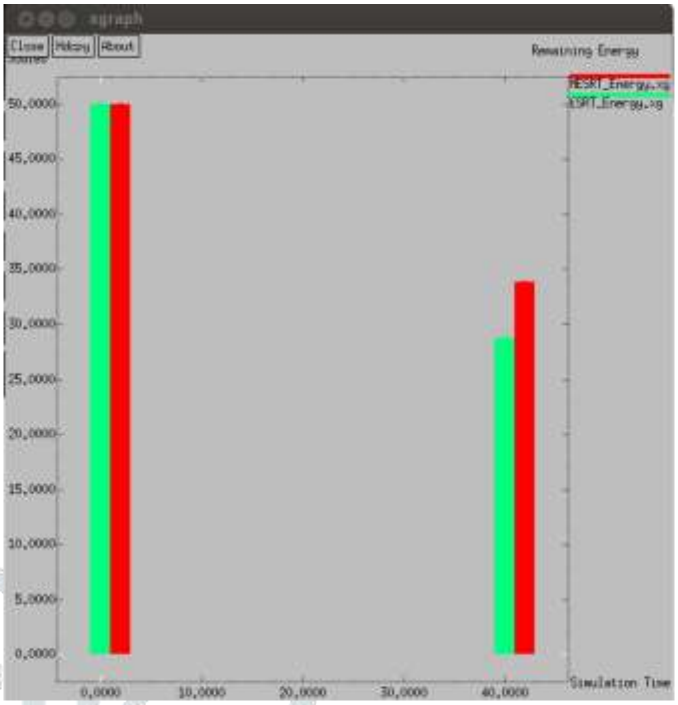

Figure 4.2: Remaining Energy Comparison

This graph shows the value of remaining energy for both the schemes. Initially the nodes have initially energy of 50 Joules. At the end of the simulation, the existing scheme had 28.73 Joules of remaining energy and modified scheme had 33.83 Joules of remaining energy. This shows that the existing scheme uses more energy in the network.

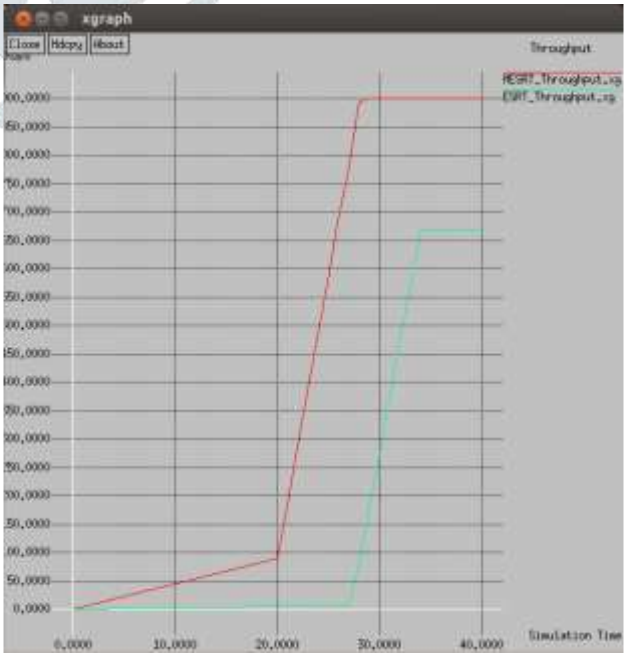

Figure 4.3: Throughput Comparison

This graph shows the comparison of the throughput for both the schemes. The value of throughput for the existing scheme was found to be 667 Kbps and for the proposed scheme, its value was found to be 901 Kbps.

Parameter\Scheme	ESRT	Modified ESRT
PDR	58.23	78.55
Remaining Energy	28.73 Joules	33.83 Joules
Throughput	667 Kbps	901 Kbps

Table 4.1: Results Comparison

V. CONCLUSION

This work was focused at modifying the trust model to detect the wormhole attack in wireless sensor network. For the existing scheme, the value of PDR shows a steep fall indicating the occurrence of attack before it gets detected eventually. When the attack occurs and the malicious node drops the packets, its trust value gets reduced. The proposed scheme however, does not allows the attack to happen. Instead the trust values are computed at the destination node after the route request phase. Once the malicious nodes are detected, the data transmission begins after that. This increases the value of packet delivery ratio for the proposed scheme. The higher value of packet delivery ratio also increases the throughput of the network. Therefore, we can conclude that the proposed scheme outperforms the existing scheme.

This proposed scheme generalizes the trust based scheme for wormhole attack. In future, the trust computation can be generalized for other attacks such as flooding attack, or denial of service attack etc.

References

1. F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," Transactions on Emerging Telecommunications Technologies, vol. 26, no. 2, pp. 107–130, 2015.

2. K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," IEEE Communications Surveys and Tutorials, vol. 14, no. 2, pp. 279–298, 2012.

3. H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proceedings of the IEEE, vol. 98, no. 10, pp. 1755–1772, 2010.

4. H. Yu, Z. Shen, C. Miao, B. An, and C. Leung, "Filtering trust opinions through reinforcement learning," Decision Support Systems, vol. 66, pp. 102–113, 2014.

5. H. Yu, Z. Shen, C. Leung, C. Miao, and V. R. Lesser, "A survey of multi-agent trust management systems," IEEE Access, vol. 1, no. 1, pp. 35–50, 2013.

6. Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Abdul Waheed Khan, Khalid Haseeb, "Energy-aware and secure routing with trust for disaster response wireless sensor network", Peer-to-Peer Networking and

Applications, January 2017, Volume 10, Issue 1, pp 216–237.

7. Jianpo Li, Dong Wang, “The Security DV-Hop Algorithm against Multiple-Wormhole-Node-Link in WSN”, Vol. 13, No.4, April 30, 2019.

8. Manish Patel, Akshai Aggarwal, Nirbhay K. Chaubey, “Detection of wormhole attacks in mobility-based wireless sensor networks”, International Journal of Communication Networks and Distributed Systems, 2018 Vol.21 No.2.

9. K. Karthigadevi, S. Balamurali and M. Venkatesulu, “Wormhole Attack Detection and Prevention Using EIGRP Protocol Based on Round Trip Time”, Journal of Cyber Security and Mobility, Vol: 7 Issue: Combined Issue 1 & 2, January 2018.

10. Ranu Shukla, Rekha Jain, P. D. Vyavahare, “Combating against wormhole attack in trust and energy aware secure routing protocol (TESRP) in wireless sensor network”, 2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE).

11. R.M. Dilip Charaan, R. Ramesh and E. Uma, “Detection and Prevention of Wormhole Attacks in Leach Protocol for Wireless Sensor Networks”, Asian Journal of Information Technology, Year: 2017, Volume: 16, Issue: 1, Page No.: 69-76.

12. A. BabuKaruppiah, G. Sri Vidhya, S. Rajaram, “An Energy Efficient Wormhole Detection Technique by Traffic Analysis in Wireless Sensor Networks”, International Journal of Engineering and Computer Science, December 2017.