The Multipath Routing and Intrusion Tolerance for Redundancy Management in Wireless Sensor Networks

Shruthi S M
M Tech 4th sem,,Dept of CS&E
Institute of Technology
Chitradurga, India

Nagabhushana
Prof., Dept of CS&E
S.J.M Institute of Technology
Chitradurga, India

***Abstract*- In this paper we propose a wireless sensor network, which is a new technology and that gathers the data from the hostile environment. The tradeoff between reliability gain v/s the energy consumption, they maximize the WSN system lifetime. For this, we determining best redundancy and also best intrusion detection system. The multipath routing provides the best communication for the nodes and also improves the load balancing and quality of service. So we are developing a novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy.**

Keywords- Wireless Sensor Network, Iintrusion Detection System, Reliability, Energy Consumption, Multipath Routing, Intrusion Tolerance.

I. INTRODCTION

The WSN's satisfies QoS requirements such as scalability, reliability, timeliness and also it minimize the energy consumption. The energy consumption is due to (1) transmitting/receiving data. (2) Processing query requests and (3) forwarding queries/data to neighboring nodes. One of the problems is the technique that is used for improving or reducing the reliability gain v/s energy consumption, they maximize the WSN system lifetime. So, to overcome this problem, clustering is the best solution and also it achieves the scalability, energy consumption, and reliability. To reduce the energy consumption, we propose a number of protocols. These protocols exploring the tradeoff between reliability gain v/s energy consumption.The WSNs are used in many applications such as military services, forest fire monitoring and also it comprises battery powered sensor nodes. The multipath routing of WSNs are often becomes target of malicious attacks. The attacker tampers the nodes physically. The wireless sensor networks contain more bandwidth compare to wired networks.

The technique for sending data in a wireless sensor network which will contain some drawbacks

- Utilization of available bandwidth is low.
- There is Traffic in communication channel.
- Efficient data transmission will not take place.
- Packet loss is more.
- Reliability of communication is low.

Intrusion detection provides some challenges to WSNs, due to the lack of resources. The methods that are used to develop the traditional networks that they are not directly applied to the WSNs, so they want the resources that are not present in the wireless sensor networks. Intrusion detection considers the behavior of a normal system that is completely different from the behavior of a system under attack.

The tradeoff between reliability gain v/s energy consumption will maximizes the WSN system lifetime. To overcome this problem, clustering is the best solution. This clustering achieves the scalability, energy consumption, and reliability. Many wireless sensor networks (WSNs) are involved in unattended environment so the energy conservation is difficult. So due to limit resources, a WSN does not satisfy the QoS requirements such as reliability, timeliness and security, scalability but it minimizes the energy consumption. The tradeoff between energy consumption v/s reliability gain should maximizes the WSN system lifetime so if we considering this tradeoff, which is not working properly with the malicious attackers.

In intrusion tolerance, we solving two problems (1) how many paths to be use and (2) what path to use. First we go the how many paths to be use problem then we go to the second problem that is what path to use. To solving these problems we are not consider the routing protocols. Rather, for energy conservation, we develop the IDS for intrusion detection is performed. The compromised nodes remove the HWSN so these compromised nodes are involved in intrusion detection to disturb the routing protocols. The first problem "how many paths to use" that tolerates the compromised nodes to maximizing the HWSN system lifetime.

In WSN, to improve the data delivery, multipath routing is an efficient mechanism for fault and intrusion tolerance. If we sending information from source to destination through multipath, if any one path reaches the destination mean the probability will be increases. The tradeoff between reliability gains vs. Energy consumption that will maximize the WSN system lifetime. To overcome this problem, clustering is the best solution and it achieves scalability, reliability, and energy consumption.

For considering the management of redundancy, data are sending from source to destination through multipath in presence of unreliable and malicious nodes. If we ignore the tradeoff between reliability gain v/s energy consumption, it will shorten the WSN system lifetime.

II. OBJECTIVE OF THE SYSTEM

The project "The management of redundancy for multipath routing and intrusion tolerance in unreliable and malicious wireless sensor network "is implemented that provides the efficient data transmission in wireless sensor networkSYSTEM ARCHITECTURE

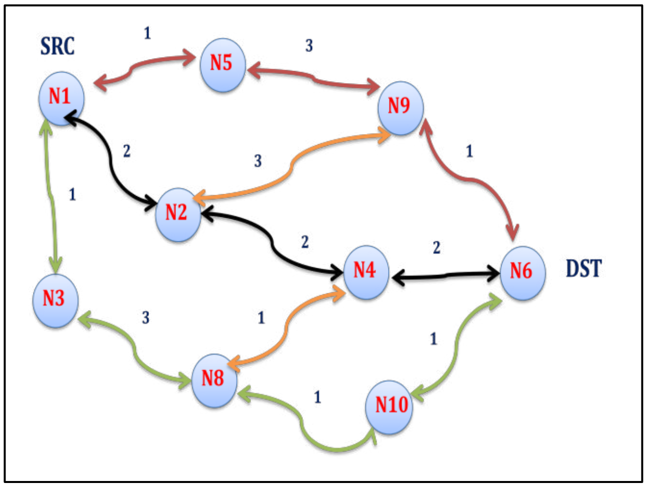

Figure 6.1: Example of a wireless sensor network

If we consider the shortest path from source node 1 to destination node 6 in figure 6.1,

N1→N5→N9→N6 = 5 (a)

After getting the shortest path (i.e., a), it will forward data to the remaining paths, if all other paths are active then only data is transmitted successfully ,which save the time and traffic and it will send data at high speed.

To overcome this problem and to make a reliable communication between source and destination and to save time and bandwidth, we consider all shortest paths from source to destination

N1→N5→N9→N6 =5
N1→N2→N9→N6 =6 N1→N5→N4→N6=6
N1→N3→N8→N10→N6 =6 N1→N3→N8→N4→N6=7

The nodes N9 and N8 are repeated in two paths, so we consider only one path that will contain shortest distance and also the throughput is 0 and also wasting of time and bandwidth.

To Overcome this we are using management of redundancy for intrusion tolerance which,

- First identifies the multiple path form source to destination.
- Arrange it according to shortest path.
- Finds the status of intermediate node active or inactive.
- make group (cluster) of Active nodes
- Find any redundancy path is present if any, remove it and kept only valid path which does not contain redundancy path
- Then send data from all available multiple paths.

III. IMPLIMENTATION

There are three modules in our project

1. Multipath routing
2. Intrusion tolerance
3. Energy efficient

1. Multipath routing- To improve the data delivery in WSN, multipath routing is an efficient mechanism in fault and intrusion tolerance. If we sending the information from source to destination through multipath, any one path that reaches the destination mean the probability will be increases. If we ignore the tradeoff between reliability gains vs. energy consumption, it will shorten the WSN system lifetime.

2. Intrusion tolerance- In this module, we solve two problems

I. How many path to be used
II. What path to use

The compromised nodes remove the HWSN so these compromised nodes are involved in intrusion detection to disturb the routing protocols. The first problem "how many paths to use" that tolerates the compromised nodes to maximizing the HWSN system lifetime. The second problem "what path to use tells about the data that reaches the destination?

3. Energy efficient- The IDS is implemented in WSN, there are two approaches

The first approach is applicable to flat WSN. Flat WSN are used in between intermediate node that feedback the malicious nodes and the energy conservation of a neighboring node to the sender node.

Another approach is to use local host-based IDS for energy conservation.

IV. ALGORITHM

Multiple shortest paths algorithm

```
Step 1: Generate a routing table.
Step 2: Find all the possible paths from
source to destination.
Step 3: Find weightage of al the calculated
possible paths.
        [Note: consider only connected paths]
Step 4: Sort the paths.
```

V. CONCLUSION

In this paper we performed a tradeoff analysis between energy consumption v/s QOS gain in reliability, timeliness, and security for redundancy management of clustered heterogeneous wireless sensor networks will maximizes the WSN system lifetime. The WSN satisfies the QoS requirements such scalability, reliability, and timeliness. If we ignore the tradeoffbetween reliability gain v/s energy consumption it will shorten the WSN system lifetime. So we developed a novel probability model to analyze the best redundancy level in terms of path redundancy (*mp*) and source redundancy (*ms*). In future work, we are using more malicious attacks for energy conservation, reliability, and scalability to investigate the intrusion detection and multipath routing based on the protocols.

VII RESULTS AND DISCUSSIONS

Finally we eliminate the redundancy path from a WSN and find out all shortest path from source to destination. This shortest path does not contain any redundancy path and shows the successful delivery of data. Once the data is delivered to the destination it clearly the shortest path that that containing shortest distance.

ACKNOWLEDGEMENT

This journal paper is made possible through the help and support from everyone, including: parents, teachers, family, friends and in essence, all conscious being. Especially, please allow me to dedicate my acknowledgement of gratitude towards the following significant adviser and contributors: First and foremost, I would like to extend my gratitude to my Project Guide and Head of the Department of Computer Science and Engineering Prof. Dr. Nagabhushana MTech., P.h.d., for his most support by providing excellent infrastructure and research facilities. Last but not the least we also thank to our Faculty members, staff and friends for being instrumental towards the completion of this paper.

REFERENCES

[1] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient,distributedclustering approach for ad hoc sensor networks," IEEE Trans. MobileComput., vol. 3, no. 4, pp. 366- 379, 2004.

[2] E. Felemban, L. Chang-Gun, and E. Ekici, "MMSPEED: multipat Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness inwireless sensor networks," IEEE Trans. Mobile Comput., vol. 5, no. 6, pp.738-754, 2006.

[3] I. R. Chen, A. P. Speer, and M. Eltoweissy, "Adaptive Fault-TolerantQoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks," IEEE Trans. on Dependable and Secure Computing, vol. 8, no. 2, pp. 161-176, 2011.

[4] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S.Singh, "Exploiting heterogeneity in sensor networks," 24th Annu. JointConfof the IEEE Computer and Communications Societies (INFOCOM), 2005, pp. 878-890 vol. 2.

[5] H.M.Ammari and S. K. Das,"Promoting Heterogeneity, Mobility, and Energy-Aware Voronoi Diagram in Wireless Sensor Networks," IEEETrans. Parallel Distrib.Syst. vol. 19, no. 7, pp. 995-1008, 2008.

[6] X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," IEEE 61st Vehicular Technology Conference, 2005, pp. 2528-2532.

[7] S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks, IEEEWirelessCommun" vol. 14, no. 5, pp. 56-63, 2007.