Intrusion and Fault Tolerance in Heterogeneous Wireless Sensor Networks Using Weighted voting Method

Gururaja N*, Dr.Brahmananda S H**

* Computer Science and Engineering, Rajiv Gandhi Institute of Technology, Bengaluru
**Computer Science and Engineering, Rajiv Gandhi Institute of Technology, Bengaluru

Abstract-A wireless sensor network (WSN) is a large collection sensor node with limited memory, battery and processing capacity. Due to this limited resources the energy conservation plays important role in wireless sensor networks. We formulate optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that query success probability maximized while prolonging system useful lifetime. In redundancy management "packet dropping" and "Bad mouthing" are the major problems in managing the redundancy. In order sort out these problems we plan to propose "weighted voting" based trust management method is used to achieve best energy efficiency. The main function of weighted voting method is to find the trust/reputation of neighbor nodes.

Index Terms- Multipath routing, Wireless Sensor Networks, Bad mouthing, security, energy conservation.

I. INTRODUCTION

THE Wireless Sensor Network provides a new prototype for sensing and disseminating information from various Environments, with the potential to serve many and diverse applications. WSN consists of a huge number of small sensor nodes that are grouped with analyzing, processing and communicating components and base station. The WSN authority can send queries to the base station and spread those queries to network. Hence base station act as a gateway between the WSN and external world. The applications of the WSN include Earth monitoring, health care monitoring, industrial monitoring etc., This feature of sensor networks makes them more susceptible to various attacks. So Wireless Sensor Networks need more security to withstand in critical areas. Cryptography and authentication approach provides security to WSN. But these approaches do not provide sufficient security in autonomous network. So a trust based methods are used for providing security to the network. For security enhancement and successful collaboration of sensor networks, trust based approach is essential.

In most wireless sensor networks (WSNs) are organized in an unrelated environment in which energy replacement is difficult if not impossible. WSN must not only satisfy the application specific QoS requirements such as timeliness, security and reliability but also minimize energy consumption to prolong the useful system lifetime. The tradeoff between consistency gain vs energy consumption with the goal to maximize the WSN system lifetime has been well explored in the literature

No prior work exists to consider the tradeoff in the presence of malicious nodes. Routing among multiple positions is to consider an good mechanism for fault and intrusion tolerance to improve data delivery in Wireless Sensor Networks. The idea for the probability of that least one path reaching the sink node or base station increases as we have more paths during delivery of the data The most prior request focused on using multiple routing to improve efficiency, some attention has been paid to using among the routing to tolerate insider attacks however, largely ignored the tradeoff between gain and QOS. Energy consumption is very short in the system lifetime. The research problem we are addressing in this paper is effective redundancy management of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes. We address the tradeoff between consumption of the energy and QoS gain in timeliness, reliability and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. Most specifically, we analyze the optimal amount of redundancy that through which data are routed to a remote sink in the presence of unreliable and malicious nodes with attackers, so that the query success ratio of the probability is maximized while maximizing the HWSN lifetime. We consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to remove malicious nodes from the HWSN. The contribution is a modeling based analysis methodology by which the optimal with multipath redundancy levels and intrusion detection settings may be identified for satisfying application QoS requirements while maximizing the lifetime of HWSNs.

In paper [1] the author has proposed based on weighted voting that allows for each local window to cast not just a single vote, but a set of weighted votes. In [2] the paper has a proposed algorithm called greedy weighted region routing (GWRR) algorithm that addresses message loss tolerability in harsh and hostile environments by assigning higher weights to harsher regions and then we present a nearly-optimal routing in dense WSNs. In another paper [3] propose to use the key techniques and probabilistic multi-path redundancy transmission (PMRT) to find out the wormhole attacks. Identification based key management scheme is used for wireless sensor networks to build security link and detect wormhole attack.

Heterogeneous wireless sensor network (HWSN) consists of sensor nodes with different ability, such as different computing power and sensing range. Compared with homogeneous WSN, the heterogeneous WSN consists of sensor nodes with different abilities, such as various sensor types and communication and sensing range, thus provides more flexibility in deployment.

For example, WSN can construct in which nodes are equipped with different kinds of sensors to provide various sensing services.

The tradeoff Performance of both energy consumption and QoS gain in both security and reliability to maximize the system lifetime and also uses the multipath routing to tolerate intrusion detection process where decision is based on a majority voting of monitoring nodes and considering energy being consumed for intrusion detection. Both cluster head (CHs) and sensor nodes (SNs) can be compromised for lifetime maximization. The basic idea is that heterogeneous wireless sensor network (HWSNs) nodes having wireless link with dissimilar communication range, sensing range, densities and capabilities. It Increases the network lifetime and reliability and energy also achieved.

Intrusion detection system (IDS) is used to detect malicious nodes. Two problems will arise:1)what paths to use and 2) how many paths to use and to overcome this problem multipath routing is used, is a routing technique of using multiple alternative paths through a network. Trust based systems are used to tackle the "what path to use" problem and here trust based intrusion detection observe the existence of optimal trust threshold for minimizing both false positive and false negative. and is used to identify the best trust formation model as well as drop dead trust is the best application level threshold under which anode is considered misbehaving to optimize the application performance in false alarm probability.

When data need to be sent from a sender to a receiver, then the data will go to the processing center. In fig: 1 which consists of cluster head which will be a random based on the success ratio with in a particular cluster. For each and every group of cluster a cluster head will be selected based on the success ratio. Then the router will maintain the multiple sensor nodes which are under them. If a sensor node is need to send some data to other sensor node. The sensor node will transmit the data to the cluster head. The router will start its work of finding the path way to the destination node. The path for the destination node is obtained by shortest distance. The path of the destination node have been found the data will be transmitted from one cluster head to another cluster head by using the nodes nearby the cluster head. Then data will be reaching the processing center where the destination point will be shown along with the data. Now processing data takes the whole responsibility of the data which has been got from the cluster head's. The data will be containing the information that is needed to be sent to a particular user and also the destination id/address. The processing center can only be able to open the destination id/address information and not the information that is to be shared with the destination.

II RESEARCH ELABORATIONS

When data need to be sent from a sender to a receiver, then the data will go to the processing center. In fig: 1 which consists of cluster head which will be a random based on the success ratio with in a particular cluster. For each and every group of cluster a cluster head will be selected based on the success ratio. Then the router will maintain the multiple sensor nodes which are under them. If a sensor node is need to send some data to other sensor node. The sensor node will transmit the data to the cluster head. The router will start its work of finding the path way to the destination node. The path for the destination node is obtained by shortest distance. The path of the destination node have been found the data will be transmitted from one cluster head to another cluster head by using the nodes nearby the cluster head. Then data will be reaching the processing center where the destination point will be shown along with the data. Now processing data takes the whole responsibility of the data which has been got from the cluster head's. The data will be containing the information that is needed to be sent to a particular user and also the destination id/address. The processing center can only be able to open the destination id/address information and not the information that is to be shared with the destination.

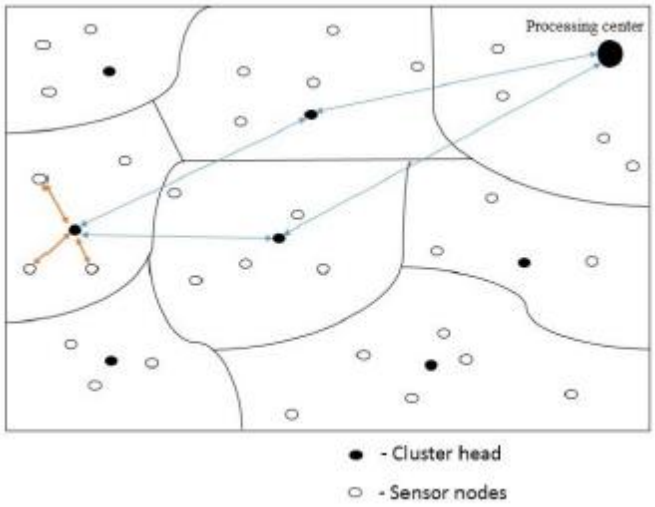

Fig 1: Packet Delivery

Now the processing data will find the destination address, and will find under which cluster head the node lies r the node itself a cluster head. After know the information about the destination point the data will be forwarded to the destination point. In the above fig:4.1 the packet delivery has been done successively, the cluster head which got the data from the nodes under. Then the cluster head which got the data, forward to the other cluster head to its way to the processing center. There the data will be forwarded to the particular node, from the processing center. When the process executes without error then nothing to be worried, but we know that the sensor nodes are wireless and will be movement, no nodes will be with stand in the same place for a long time so the data which has to be sent may sent twice as because the node moves from one cluster group to another cluster group. The PS will check the data and result that the data has been already sent and the data will be sent again to the cluster group nodes, which forwarded to the PS. There a process called

Packet drop must be done. If the process of packet drop has been done then the node is not a malicious or an intruder.

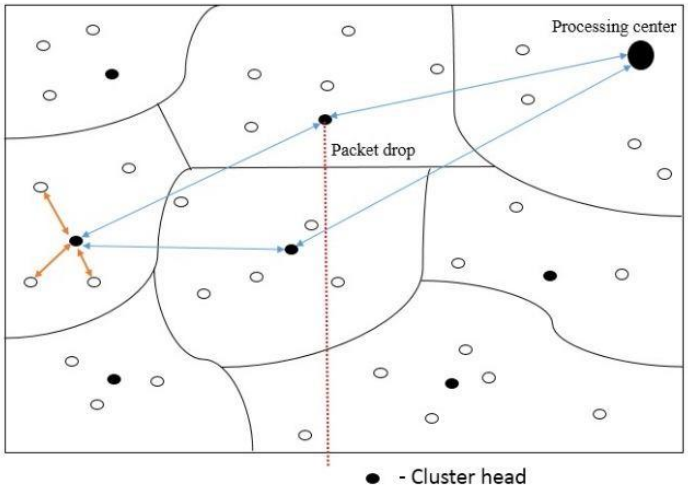

Fig 2: Packet Drop

In fig 2 packet Drop we can see that the data has been sent twice and the processing center has again sent the data to the cluster which has forwarded the packet to processing center. There the packet drop process has been done successively. And know that the information has not be stolen and seen by other node.

The packet will be dropped by the cluster head, when the data has been already sent. If the packet has not been dropped then the cluster head or the node which did not drop the packet behaves as a malicious node. The function of no dropping the packet is called as Bad Mouthing. This becomes the main problem when in the redundancy, wireless sensor networks. When some nodes in a cluster group need to send some data to other cluster node. The nodes which need to send information will approach the cluster head of its group, and then the data will be sent to the cluster head. Each and every cluster will have direct connection or an indirect connection to processing head. Now the cluster head will get the data and send the data to the processing head. As the cluster nodes and head will be in movement the data can be sent more than one time. When the data reaches the processing head the information will be checked and will be sent to the particular node destination.

As like the before process the data will be reaching the processing head, the PC (processing center) will analyze the data, and identifies the data has been sent already to the respective destination node. So the PH will send the data again to a cluster head with the information that the data has been already sent. Now the data must reach the original sender node as the data has been already sent, so the processing Center will forward the data to the cluster heads, and from the cluster head the data will be forwarded to the respective cluster node. Suppose the data did not reach the source then the data must be dropped by some cluster head. If did not then "Bad Mouthing" affects. This problem can be overcomes by using the proposed technique called "weighted based voting'.

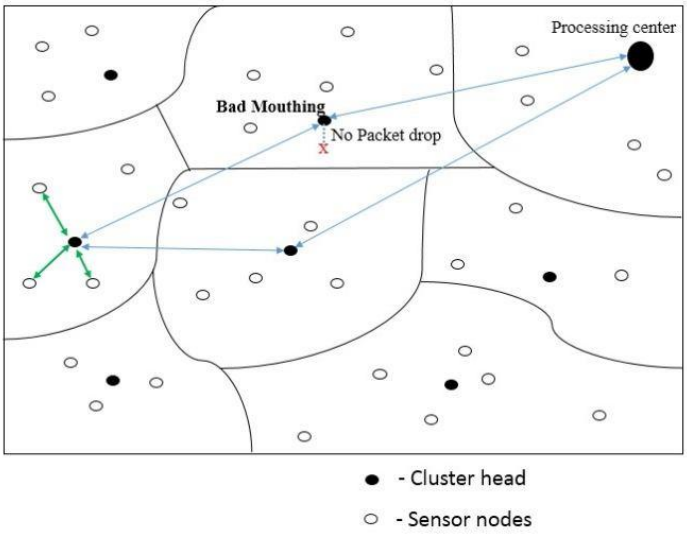

Fig 3: Bad mouthing

In the above diagram we can view the occurrence of the "Bad mouthing" attack, and also no packet drop by the cluster head After getting the data from the processing center. This attack only occurs due to the movement of the cluster nodes. The movement of the cluster nodes cannot be stopped and should not be done. So the problem of 'bad mouthing' can be stopped by using the weighted based voting.

As discussed before the problem of "bad mouthing became an issue in wireless sensor network, this attack occurs mainly in cluster based routing and uses takes the data or information of other node, when packet drop need to be done. To remove malicious nodes from the system, a voting based distributed IDS is applied periodically in every time interval. A CH is being assessed by its neighbor CHs, and a SN is being assessed by its neighbor SNs. In each interval, m neighbor nodes (at the CH or SN level) around a target node will be chosen randomly as voters and each cast their votes based on their host IDS results to collectively decide if the target node is still a good node. The m voters share their votes through secure transmission using their pair wise keys.

When the majority of voters come to the conclusion that a target node is bad, then the target node is evicted. For both CHs and SNs, there is a system-level false positive probability that the voters can incorrectly identify a good node as a bad node. There is also a system-level false negative probability that the voters can incorrectly misidentify a bad node as a good node. These two system-level IDS probabilities will be derived based on the bad-mouthing attack model in the paper. Assume that the capture time of a SN follows a distribution function Fc(t) which can be determined based on historical data and knowledge about the target application environment.

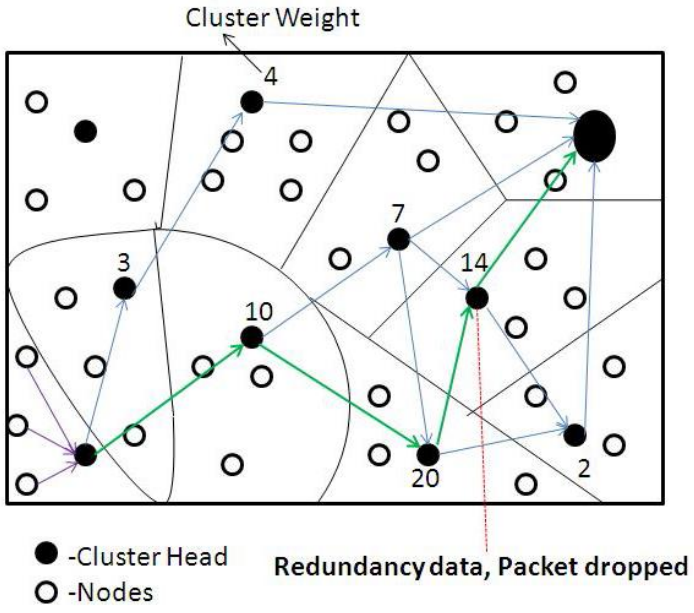

Fig 4: Weighted Based Voting

In the above diagram, the nodes in a particular cluster are in need to send some data or information to a destination. Then now by using the proposed scheme of Weighted based voting, the process begins with the weighting of cluster heads. The head which has a highest weight will be having high successive rate. So the data will be sent to the particular cluster head to processing center. While the cluster head get the same data twice the packet drop will be as a redundancy data. Here a cluster head sends a data and using weighted voting it selects the cluster head which has a weight "10", and from there again the process of weighted voting begins of selecting the cluster head now heads has the values "7", "20". So by selecting highest weight the data travels through weight "20". And then "14" then to the processing head.

Then, the probability that a SN is compromised at time t, given that it was a good node at time t, denoted by 1, is given by: We note that _1 is time dependent. For the special case in which the capture time is exponential distributed with rate λc,_1 = 1 − 2345×789:.Recallthat the voting-based distributed IDS executes periodically with being the interval. At the ith IDS execution time (denoted by), a good node may have been compromised with probability1 since the previous IDS Execution time.

III CONCLUSION

As many attacks like the "bad mouthing" are approaching to attack the wireless sensor network. We are in need to get prepare For the attacks to be rectified. As like as the same in this paper the Bad mouthing attack has been controlled by using weighted based voting method which has been proposed in this paper. In future this bad mouthing will itself attack in different form or will get newer version, so the rectification is also needed to be updated "higher weight based voting.

REFERENCES

[1] Jain, A. K. (2000). "Statistical Pattern Recognition: A Review", IEEE Transactions on pattern analysis and machine intelligence, 22, no.1.

[2] Bishop, C. (1995). Neural networks for Pattern Recognition, Oxford University Press, New York.

[3] Turk, M., A., Pentland, A., P. (1991). "Eigenfaces for Recognition", J. Cogitative Neuroscience, 3, no. 1.

[4] Belhumeur, P. N., Hespanha, J. P., and Kriegman, D. J (1997). "Eigenfaces vs. Fisherfaces: recognition using class specific linear projection",Pattern Analysis and Machine Intelligence, IEEE Transactions on , 19, Issue: 7 , 711-720.

[5] Wiskott, L., Fellous, J. Kruger, M., N., and Malsburg, C. von der (1997). "Face Recognition by Elastic Bunch Graph Matching", IEEE Transactions on PatternAnalysis and Machine Intelligence, 19,. Issue 7, 775-779.

[6] Kaneko, S., Satoh, Y., and Satoru, Igarashi (2003). "Using selective correlation coefficient for robust image registration", Pattern Recognition,36, Issue 5, 1165-1173.

[7] Combining Local Similarity Measures: Summing, Voting, and Weighted Voting. Paul watta, mohammadJ.Hassoun, IEEE transation.

[8] GWRR: Greedy Weighted Region Routing in Wireless Sensor Networks EuhannaGhadimia, Nasser Yazdania, Ahmad Khonsaria,2008 14IEEE International Conference on Parallel and Distributed Systems.

[9] Detecting Wormhole Attacks Using Probabilistic Routing and RedundancyTransmission,Guiyi Wei, Xueli Wang, 2010 InternationalConference on Multimedia Information Networking and Security.

AUTHORS

First Author -Gururaja N has received his B.E degree in Computer Science and Engineering from Dayananda Sagar College of Engineering, VTU University in 2010.he is pursuing M.Tech in Computer Science and Engineering from Rajiv Gandhi Institute of Technology, Bengaluru.
E-mail: gururaja402@gmail.com

Second Author – Dr. Brahmananda S H, Professor and HOD in Department of Computer Science and Engineering @ Rajiv Gandhi Institute of Technology Bengaluru.