INTRUSION DETECTION IN HETEROGENEOUS NETWORK BY MULTIPATH ROUTING BASED TOLERNENCE PROTOCOL

S. Dinesh Kumar[1], A.Thillipan[2], L.Karthikeyan[3]

[1]PG Student, M.E (CSE), [3]Asst.Professor, Dept of CSE, Valliammiai Engineering college, Chennai, India.
[2]PG Student, M.E (Embedded Systems), CMS College of Engineering, Namakkal, India

Abstract

The key theory of our redundancy management is to achieve the tradeoff between energy consumption vs. the gain in timeliness, security, and reliability to increase the system useful lifetime. A Innovative probability model to analyze the best redundancy level in terms of source redundancy, path redundancy and as well as the best intrusion detection settings in terms of the number of voters and the intrusion invocation break under which the lifetime of a HWSN [Heterogeneous Wireless Sensor Network] is maximized. In redundancy management "badmouthing" is the major problem in managing the redundancy. This badmouthing is malicious node which will never drop the packet even after knowing that the packet has been sent already. In this paper we propose a new scheme to overcome the problem of badmouthing by weighted based voting, this protocol will weight (Success Rate) all the nodes in the network to find the non-malicious node in the network which having more packet drop. In "weighted voting" main function is to find trust/reputation of neighbor nodes, as well as to tackle the "what paths to use" problem in multipath routing decision making for intrusion tolerance in WSNs.

Keywords: *Bad mouthing, Wireless Sensor Network, Weighted Based Voting, HWSN.*

----------***----------

1. INTRODUCTION

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 position is to considered 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.

2. RELATED WORK

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.

2. ORGANIZATION OF PAPER

We have passed away from abstract which give the overview and also say about the main concept of the paper. In section I, served with a brief and clear introduction about the WSN and redundancy progress. In session II, Literature survey gone through has been given as related work. In session III, the system in present, which is given as existing system? In session IV, this Concept will be given as Proposed System. Session V had the conclusion. Final Session finishes the paper with the future work that can be possibly done.

3. EXISTING SYSTEM

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 consist 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 need 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.

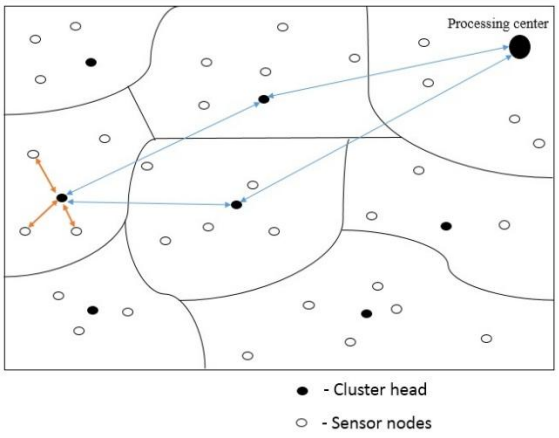

Fig 1: Packet delivery

Now the processing data (PD) will find the receiver address, it will find under which cluster head the node lies r the node itself a head of the cluster. The information about the destination point the data will be forwarded to the destination point. The packet delivery has been done successively, the router which got the data from the nodes under. Then the cluster head which got the data, forward to the other head to its way to 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. When the data which has been sent twice, that data will be also reach the processing center (PS), there the PS will check the data and result that the data has been already sent and the data will be sent again the group of the clusters, 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.

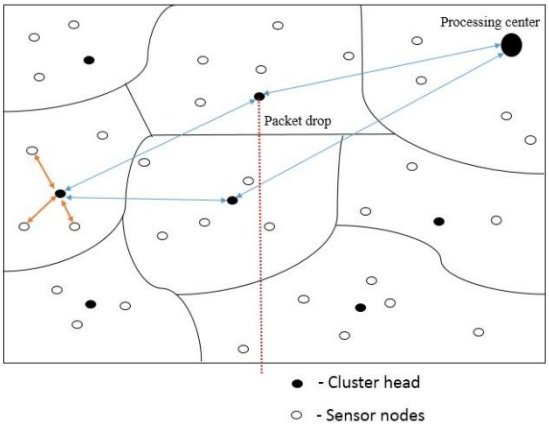

Fig 2: Packet Drop

In fig: 2 packet drop, we can c 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. The packet drop for process has been done successfully and knows that the information has not be stolen and seen by other node.

4. PROBLEM DEFINITION

The packet will be dropped by head of the cluster, 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 Bad Mouthing. This is a 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 the then the data has been sent to head of the cluster. Each and every cluster will have direct connection or

an indirect connection to process through the cluster head. Now , head of the cluster will get the data and send the data to the head processor. 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.
Now consider the information has been sent twice due to the movement in the cluster nodes and heads. 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 receiver node. So the data will send the data again and again to a cluster head with the information that the data has been sent already . The data must reach the particular sender node as the data has been already sent, so the processing Center can forward the data to the cluster heads, and from the cluster head the data will be forwarded to the respective cluster node. It Supposes the data did not reach the source then the data must be dropped by some cluster head. It defects if did not then "Bad Mouthing" affects. In this problem can be overcomes by using the proposed technique called "weighted based voting'.

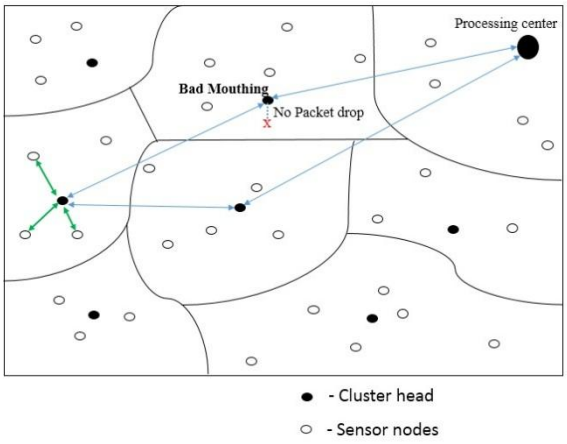

Fig 3: Bad Mouthing

In the above diagram we can view the occurrence of the "Bad mouthing" attack with no packet drop by the cluster head after getting the data from the processing center. In 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 mechanism.

5. PROBLEM SOLUTION

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 voter based distributed IDS is applied periodically in every time interval. A Cluster Head is being assessed by its neighbor Cluster Head is being assessed by its neighbor SNs. In each interval, m 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 targeted. Both the Cluster Head and Sensor Nodes, 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 probability for system function that the voters can incorrectly misidentify a bad node as a good node. There are 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.

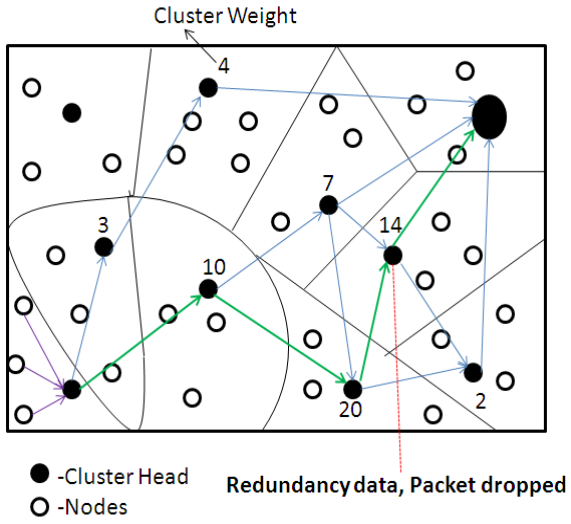

Fig 4: Weighted based voting

In the above diagram, the nodes in a particular cluster are in need to send some data or information to a destination. The proposed scheme of Weight based voting, the process begins with the weighting head for the cluster. 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.

6. CONCLUSIONS

As many attacks like the "bad mouthing" are approaching to attack the wireless sensor network. We need to get prepare for the attacks to be rectified. 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 attack itself in different form or will get new 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 transaction.

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

[9]. Detecting Wormhole Attacks Using Probabilistic Routing and Redundancy Transmission, Guiyi Wei, Xueli Wang, 2010 International Conference on Multimedia Information Networking and Security.