ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Multipath Routing for Redundancy Management in Mobile Ad-hoc Networks

A. Thillipan, S. Dinesh Kumar

PG Student, M.E (Embedded Systems), CMS College of Engineering, Namakkal, Tamilnadu, India[1]

PG Student, M.E (CSE), Valliammai Engineering College, Chennai, Tamilnadu, India[2]

ABSTRACT - In this paper we propose redundancy management by utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes with hacker nodes for analysis. It encloses the redundancy management is to exploit the tradeoff between energy consumption and the gain in reliability, timeliness, and security. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. Although the ongoing trend is to adopt by the mobile ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. Unlike the conventional network, another feature of the open network as well as closed network environment where nodes can join and leave the network freely. To analyze the best redundancy level in terms of path redundancy and source redundancy.

KEYWORDS – Wireless Sensor Network, Multipath Routing, Security, Energy Conversion

I. INTRODUCTION

In most wireless sensor networks (WSNs) are organized in an unrelated environment in which energy replacement is difficult if not impossible. Due to incomplete resources, a WSN must not only satisfy the application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to prolong the system useful lifetime. The tradeoff between energy consumption vs. consistency gain with the goal to maximize the WSN system lifetime has been well explored in the literature. However, no prior work exists to consider the tradeoff in the presence of malicious attackers. Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSN. The basic idea is that the probability of at least one path reaching the sink node or base station increases as we have more paths doing data delivery. While most prior research focused on using multipath routing to improve reliability [2,3,13], some attention has been paid to using multipath routing to tolerate insider attacks [14-16]. These studies, however, largely ignored the tradeoff between QoS gain vs. energy consumption which can adversely shorten the system life time. 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 energy consumption vs. QoS gain in reliability, timeliness and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. More specifically, we analyze the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime. Our contribution is a model-based analysis methodology by which the optimal multipath redundancy levels and intrusion detection settings may be identified for satisfying application QoS requirements while maximizing the lifetime of HWSNs.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

II. 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 WSN. In another paper [3] propose to use the key techniques and probabilistic multi-path redundancy transmission (PMRT) to detect wormhole attacks. Id-based key management scheme is used for wireless sensor networks to build security link and detect wormhole attack.

III. 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, system which is in present, is given as existing system. In session IV, the proposed Concept will be given as Proposed System. Session V has the conclusion. Session VI finishes the paper with the future work that can be possibly done.

IV. EXISTING SYSTEM

When data need to be sent from a sender to a destination, then the data must go through the processing center. In fig:4.1 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 cluster head will maintain the sensor nodes which are under them. When a sensor node is in need to send some data to other sensor node. The sensor node will transmit the data to the cluster head. The cluster head will start its work of finding the path way to the destination node. The path for the destination node is obtained by shortest distance. When the path for the destination node has 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.

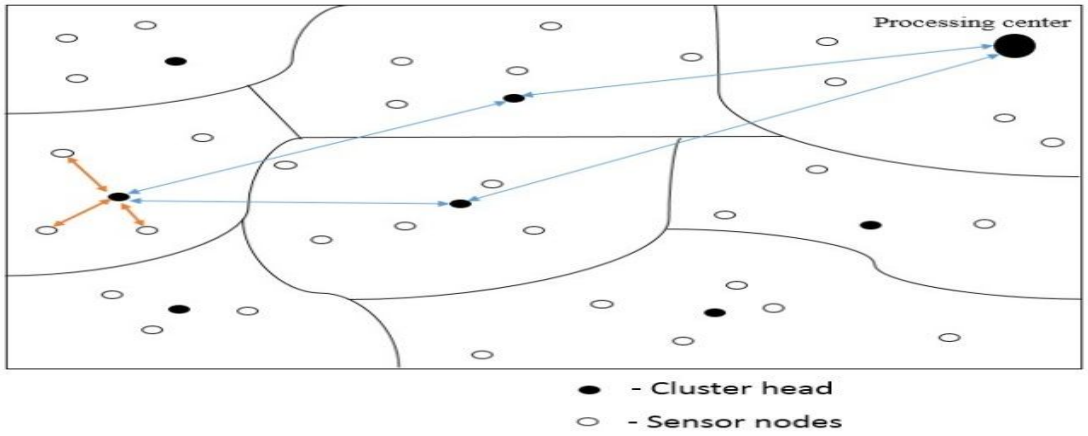

Fig 4.1: Packet delivery

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Now the processing data (PD) 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.

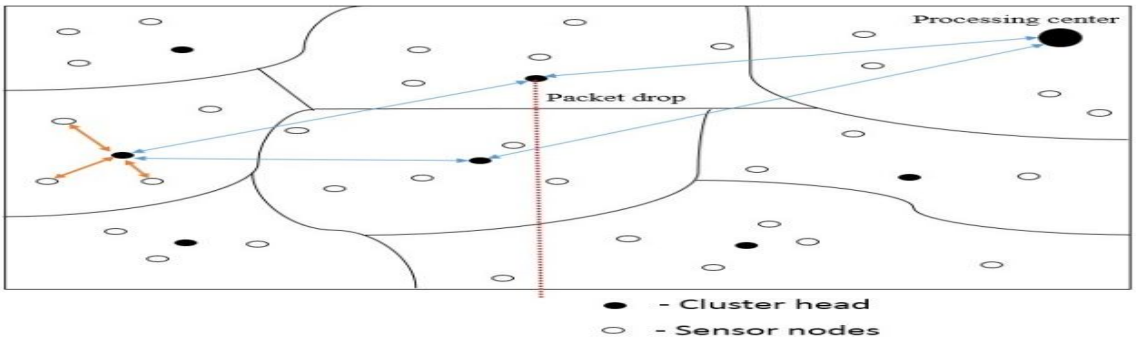

Fig 4.2: Packet Drop

In fig:4.2 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. There the packet drop process has been done successively. And know that the information has not be stolen and seen by other node.

V. PROBLEM DEFINITION

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 node which need to send information will approach the cluster head of its group, 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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'.

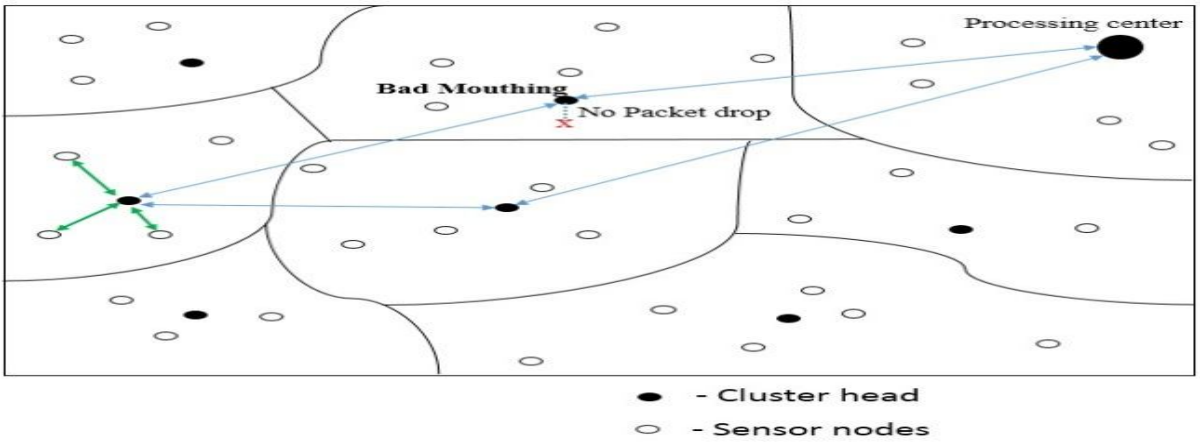

Fig : Bad Mouthing

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.

VI. 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 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 goodnode. 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

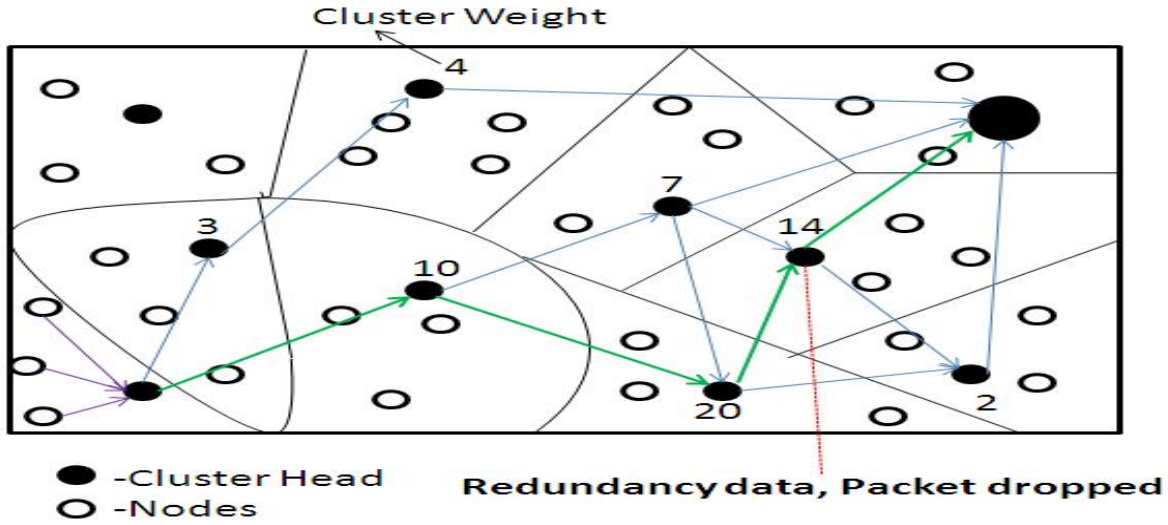

Fig: Weighted based voting

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:. Recall that 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.

VII. 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.

REFERENCED

[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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[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 14th IEEE International Conference on Parallel and Distributed Systems.

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