Redundancy Management and Energy Conservation of WSN using Multi-hop Routing and Intrusion Detection

Sanghavi N. Parkhi
Computer Science and Engineering
GHRIETW
Nagpur, India
parkhisanghavi@gmail.com

Hemlata Dakhore
Computer Science and Engineering
GHRIETW
Nagpur, India
parkhisanghavi@gmail.com

Abstract— In this paper, we will propose redundancy management of wireless sensor networks (WSNs), using multihop routing to answer user queries in the existence of unreliable and malicious nodes. The key concept behind our redundancy management is to exploit the balancing between energy consumption vs. promptness, and security to increase the system lifetime. We will use an algorithm for Redundancy Management for identifying the best redundancy level in wsn to apply to multihop routing for intrusion tolerance, and to increase the query success probability of system lifetime. We will develop a new probability model to analyze the best redundancy level in terms of multiple path redundancy and multiple source redundancy, and also the best intrusion under which the lifetime of a WSN is increased. To increase the WSN lifetime, we will calculate the Lwsn value by capturing the radio ranges and apply the analysis results to a particular redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes. A prototype implementation in the java simulator will be used to demonstrate malicious attacks launched by intruder node.

Keywords- WSN, multi-hop routing, promptness, security, energy consumption, Intrusion Detection, Lifetime.

*****

I. INTRODUCTION

Wireless sensor networks (WSNs) are very expeditiously emerging as new area for various researches. Applications of WSNs are numerous and growing rapidly from indoor deployment structure in the home and office to outdoor deployment scenarios in natural, military and embedded environments. Wireless sensor network (WSN) is a group of distributed sensors and clusters which are in existence and used for monitoring and recording the physical conditions of the environment. Many wireless sensor networks (WSNs) are established in an environment which is unattended and their recovering of energy is difficult even sometimes it is impossible. Therefore, It should satisfy the promptness, reliability and security issues. Wireless Sensor Networks run critical applications and need to be protected against various malicious attacks and faults. The balancing between energy consumption vs. promptness with the goal to increase the WSN system lifetime has been well explored in the literature. Energy Efficiency is needed in WSN to ensure the network performance and prolong network lifetime. According to various researches clustering is considered as an effective solution for achieving scalability, energy conservation, and reliability. In this there will be multiple Cluster Heads(*CHeads*) and Sensor Nodes(*SNodes*) connected in a network. Which uses homogeneous nodes which rotate among themselves in the roles of cluster heads. In heterogeneous WSN environments *CHeads* nodes may take a more critical role in gathering and routing sensing data due to which there may exist a balancing issue between energy consumption and promptness and may also the complication if any malicious nodes are detected and the path will be broken.

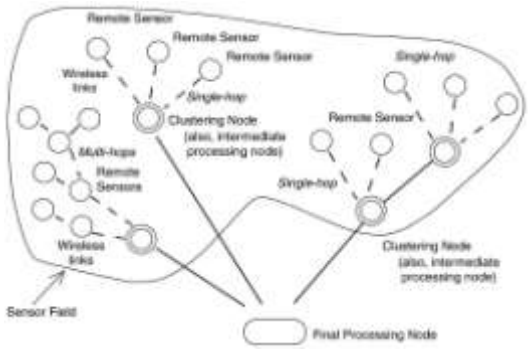

Fig 1: Typical WSN

Thus, the system will employ an intrusion detection system (*IDS*) with the goal to detect and remove malicious nodes. In most prior research focus was on using multipath routing to improve reliability, some attention has been paid while using multihop routing to tolerate inside attackers.

II. LITERATURE REVIEW

In the paper [1] redundancy management of heterogeneous wireless sensor network (HWSNs), is used for multipath routing to answer user queries in the presence of unreliable and malicious nodes. They had formulated the tradeoff as on optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance. A voting-based distributed intrusion detection algorithm was applied to detect malicious nodes in a HWSN. They had developed a new probability model to find the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection according to the number of voters and the intrusion invocation interval under which the lifetime of a HWSN is increased.

In the paper [2] the detail review of an INtrusion-tolerant routing protocol for wireless SEnsor Networks (INSENS) is been described. INSENS is used to construct forwarding tables at each node to facilitate communication between sensor nodes and a base station.INSENS not only rely on detecting intrusions, but also tolerates the intrusion by bypassing the malicious nodes. One of the important property of INSENS is that, even if a malicious node will be able to compromise a small number of nodes in its proximity, it cannot cause widespread damage in the network.

In the paper, Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection, Fenye Bao, Ing-Ray Chen, Moon Jeong Chang, and Jin-Hee Cho had illustrated the detail review of highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) which was used to effectively deal with selfish or malicious nodes. To demonstrate the utility of their hierarchical trust management protocol, they had applied it to trust-based geographic routing and trust-based intrusion detection. Trust-based intrusion detection was considered because of its elasticity against uncertainty and resiliency against attacks. They proposed an intrusion detection mechanism based on trust for mobile ad hoc networks (MANETs). They had employed the concepts of evidence chain and trust variation to evaluate a node in the network, with the evidence chain identifying misbehaviors of a node, and the trust variation reflecting the high variability of a node's trust value over a time period. In the paper,[4]Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes ,Tao Shu, Sisi Liu, and Marwan Krunz. had illustrated in detail review of an mechanisms that generate randomized multipath routes. Under their design, the routes taken by the "shares" of different packets change over time. Depending on the type of information available to a sensor, they developed four distributed schemes for propagating information .

III. PROPOSED METHODOLOGY

A Cluster Based Wireless Sensor Network (WSN) consists of various sensing nodes which are deployed in a remote region. It is susceptible to various types of attacks like sinkhole, Sybil, packet alteration, bad mouthing etc. In observation we found that existing Intrusion Detection Systems cannot resist to the overall attacks and has some limitations like it has high false positive rate and low detection rate. Also, they are not capable to detect unknown attacks. Hence, it degrades the performance of the system and consume more Energy.It is essential to design the energy efficient Intrusion Detection Systems and an efficient multipath routing mechanism to increase the lifetime of WSN. As, the sensor nodes consumes more energy in Intrusion Detection System. Following are the proposed research plan of work:

- To detect intrusion through packets in the Wireless Sensor Network and identify it as normal or abnormal packets.
- To identifying the type/nature of the intrusion/attacks by analyzing the abnormal packets according to their behavior.
- To prevent demolition of the system by raising an alarm before the intruder starts to attack.
- To explore more extensive and demolitive malicious attacks in WSN, each with different implications to energy, security and reliability.

TABLE 1
NOTATION OF SYMBOLS

Symbol	Meaning
WSN	Wireless Sensor Network
CHeads	Cluster Heads
SNodes	Sensor Nodes
Lwsn	Lifetime of wireless Sensor Network
PCe	Processing Center
Trq	Promptness Requirement
n	nodes
q	querry
mpp	Multiple path redundancy
msp	Multiple source redundancy
Tids	Intrusion Detection Interval
Nq	Maximum number of queries before energy exhaustion
Hfp	false positive probability
Hfn	false negative probability
πq	Querry arrival rate
Sq(tq,a)	Querry success probability

A. Clustering Technique:

For Clustering we had used K-means algorithm in which network is divided into number of clusters, i.e, number of nodes of a network. Nodes are assigned to the cluster having minimum distance to the cluster head *CHead* having maximum energy. The distance between the nodes is calculated using Euclidean Distance Formula. We calculate the intra cluster and inter cluster distance. And also the end toend delay of packet transmission, energy consumption for the transmission. Initially, we check how much we can lower the energy consumption by placing the *CHeads* over the network.

B. Redundancy Management:

Redundancy management of multihop routing is achieved through two forms of redundancy: source redundancy by which multiple source (*mps*) and the *SNodes* sensing a physical phenomenon in the similar feature zone are used to forward sensing data to their *CHeads* (referred to as the source *CHeads*); path redundancy by which multiple paths (*mpp*) are used to relay packets from the souce *CHeads* to the *PCe* through itermediate *CHeads*.

For redundancy management, we create *multiple* paths between the source *CHead* and the Processing center i.e, Pce for *path redundancy*. The *multiple* paths are generated by choosing *mp* CHeads in the first hop and then choosing only one CHead in each of the succeeding hops. The source *CHead*

will fail to deliver data to the Processing center if one of the following happens: (a) none of the CHeads in the first hop receives the message; (b) In the first hop, *i* ($1 \leq i < mp$) *CHeads* receive the message, and each of them attempts to form a path for delivery of data; however, all *i* paths fail to deliver the message because the succeeding hops fail to receive the broadcast message; or (c) in the first hop, at least *multiple path CHeads* receive the message from the source CHeads from which *multiple path CHeads* are randomly selected to forward data, but all *mp* paths fail to deliver the message because the succeeding hops fail to receive the message.

Algorithm for CHead and SNode Execution

1) *CHead Execution*
2) *if event is T timer then*
3) *determine radio rancge to maintain CHead i.e rCH connectivity*
4) *determine optimal Tids, m, mpp,mps by table lookup based on the current estimated density, CHead radio range and compromise rate*
5) *Notify the SNodes within the cluster of the new*
6) *optimal settings of Tids and m*
7) *else if event is querry arrival then*
8) *trigger multipath routing using multiple source ms and multiple path mp*
9) *else if event is Tclustering timer then*
10) *perform clustering*
11) *else if evemt is Tids timer then*
12) *For each neighbour CHead*
13) *if selected as an static then*
14) *execute technique for intrusion detection else// event is data packet arrival follow multihop routing protocol desing to route the data packet using AODV*

Fig: CHead Execution for redundancy management

1) *SNode Execution*
2) *Get next event*
3) *if event is T timer then*
4) *determine radio range to maintain SNode i.e rSN connectivity within a cluster*
5) *else if event is control packet arrival from CHead then*
6) *change the optimal settings of Tids and m*
7) *else if event is Tclustering timer then*
8) *perform clustering*
9) *else if event is Tids timer then*
10) *For each nieghbor SNode*
11) *if selected as an static then*
12) *execute technique for intrusion detection*
13) *else//event is data packt arrival follow multihop routing protocol design to route the data packet*

Fig: SNode Execution for redundancy mangement

C. Energy Conservation:

In this, we had used the concept of duty cycle for energy conservation. Duty cycling is mainly focused on the networking system. The most effective operation of energy-conserving is putting the radio transceiver i.e, nodes in the wireless sensor network in the (low-power) sleep mode whenever communication is not required. Specifically, the radio should be switched off as soon as there is no more data to send/recieve,and should be resumed as soon as new data packet becomes ready. In this way depending on network activities the nodes alternate between active and sleep modes depending on network activities. As sensor nodes perform a collective task, they need to synchronize with their sleep/wakeup times. A sleep/wakeup scheduling thus accompanies any duty cycling scheme. It is typically based on which sensor nodes decide when to transition from active to sleep, and back. At the same time, It allows neighboring nodes to be active for packet exchange even when nodes operate with a low duty cycle (i.e., they sleep for most of the time).

It has been observed that the number of edge-disjoint paths between nodes is equal to the average node degree with a very high probability .Therefore, whenever the density is sufficiently high such that the average number of one-hop neighbors is sufficiently larger than *m*pp and *mps*, effectively results in *mpp* redundant paths for path redundancy and mps specific paths from *mps* sensors for source redundancy.The each WSN location of the destination node needs to be known to correctly forward a packet. In clustering, a *CHead* knows the locations of SNodes within its cluster, and vice versa. A *CHeads* also knows the location of neighbor *CHeads* to the direction towards the processing center *PCe*.We assume that sensors operate in power saving mode [7] *Snodes* are either active (transmitting or receiving) or in sleep mode.

D. Routing:

Environment conditions which may cause failure of a node with a certain probability includes hardware failure (*h*), and transmission failure due to noise and interference (*n&i*). Moreover, the violence to the WSN is characterized by a per-node capture rate. Queries can be issued by the user and can be issued anywhere in the WSN through a nearby *CHeads*. A *CHead* which takes a query to process is called a query processing center(*PCe*). The AODV nodes forward the message, and record the node that they hear, creating an outburst of temporary routes back to the needy node. After receiving a message if a node and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The nodes then began sending the packets considering the route that has the least number of hops. The selection of the route from source to destination is based on query and reply cycles and various intermediate nodes store the route information in the form of route table entries along the route[4] the various control

messages are Request(Rreq), Reply(Rrep),Route Error Message(Rerr) and HELLO messages.

E. Lifetime Calculation(Lwsn):

In this *mpp*(multiple path redundancy), *msp* (multiple source redundancy and *Tids*(the intrusion detection interval) were taken as design parameters whose values were identified to increase *Lwsn* i.e., lifetime of WSN , when a set of input parameter and environmental conditions are given. we compute *Lwsn* as the average of the number of queries the system can handle without experiencing any deadline, transmission, or security failure. To calculate the *Lwsn* we consider the two design tradeoffs, we define the total number of queries that the system can answer correctly until it fails as the *lifetime* (Lwsn) of the system. A failure may occurs when no response is received before the deadline of the query.

IV. PROBABILITY MODEL

In this, we develop a probability model to estimate the lifetime of a WSN using multihop data forwarding to answer the queries issued from a user roaming in the WSN area. Table I provides the physical meanings of the notation used for symbols. We use the same notation for both *CHeads* and *SNodes*, e.g., *Pfp* and *Pfn*. While monitoring due to deformity of noise in environment or channel error is modeled by a "host" false positive probability (*Hfp*) and a "host" false negative probability (*Hfn*) which are assumed known at deployment time.

A parameter is labeled and considered as *input*, *derived*, *design* or *output*. In particular, *mpp* (path redundancy), *msp* (source redundancy), and *TIDS* (the intrusion detection interval) are design parameters whose values are to be identified to maximize *Lwsn*, when given a set of input parameter values charactering the operational and environmental conditions. Input parameters are derived from the Derived parameters. There is only one output parameter named as, *Lwsn*. Most of the derived parameters are dynamic, as a function of time. For example,density of nodes denoted by $\lambda(t)$ decreases over time because of node failure as time progresses. On the other hand, the radio ranges for *CHeads* and *SNodes*, denoted by *rCH* and *rSN*, increase over time to maintain network connectivity.

The basic idea of our lifetime i.e, WSN formulation is that we first deduce the maximum number of queries, *q*, the system can possibly handle before running into energy exhaustion, in which all queries are processed successfully. Because the system evolves constantly, the amount of energy spent per query also varies dynamically. Given the query arrival rate πq as input, the average interval between query arrivals is $1/\pi q$. So we can estimate the amount of energy spent due to query processing and intrusion detection for query *a* based on the query arrival time tq,a. Next we derive the corresponding query success probability *Sq* (*tq,q*), that is, the probability that the response to query *q* arriving at time *tq,q* is delivered successfully to the PCe before the query deadline expires. Finally, we compute *Lwsn* as the probability-weighted average of the number of queries the system can handle without experiencing any deadline, transmission, or security failure.

More specifically, the Lwsn is computed by:

$$\text{Lwsn}=\sum_{i=1}^{n}{}_{i}\left(\prod_{q=1}^{i}\text{Sq}\,(\text{tq},\text{q})\right)\left(1-\text{Sq}(\text{tq},\text{i}+1)\right)+\text{Nq}\prod_{q=1}^{i}\text{Sq}(\text{tq},\text{q})$$

where, $\left(\prod_{q=1}^{i}\text{Sq}\,(\text{tq},\text{q})\right)\left(1-\text{Sq}(\text{tq},\text{i}+1)\right)$

is used for the probability of the system which is able to successfully execute *i* consecutive queries but failure of the *i* + 1th query. The second term is for the case in which all queries are processed successfully without experiencing any failure which will have system with the longest lifetime span.

V. EXPERIMENTAL SETUP

The snapshots of experimental setup are as follows :

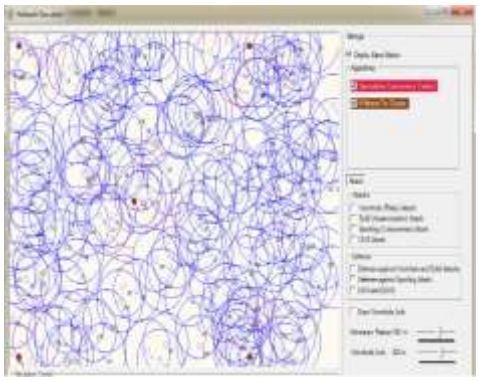

Fig 1: Screenshot of Deploying a network using network simulator

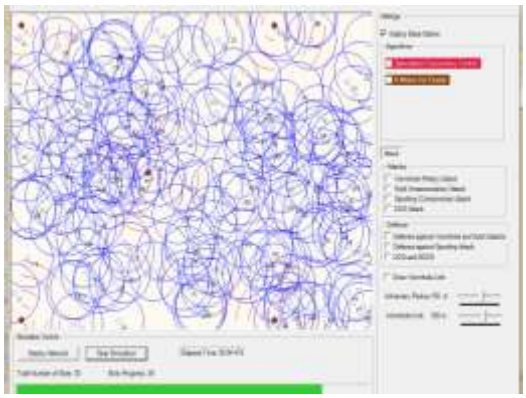

Fig 2: Screenshot of Start of simulation in deployed network

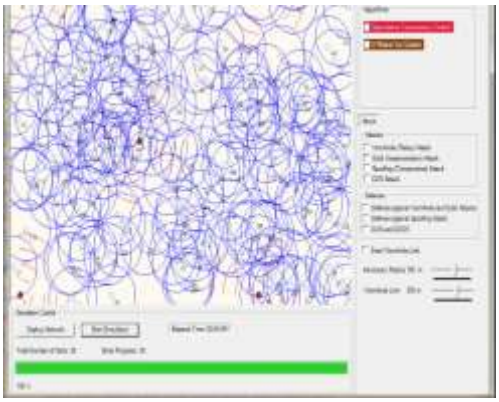

Fig 3: Screenshot of Stopping simulation in deployed network

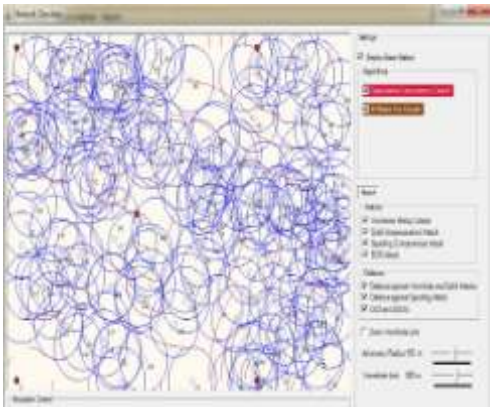

Fig 4: Screenshot of simulation of various attacks and its defense.

VI. CONCLUSION

In this paper, we had performed a balance analysis of energy consumption vs. promptness, and security for redundancy management of clustered wireless sensor networks (*WSN*) by utilizing multihop routing and trust-based intrusion detection to answer user queries. We had developed a probability model to analyze the best redundancy level in terms of both path redundancy (*mpp*) ,source redundancy (*mps*), and the intrusion invocation interval (*Tids*) under which the lifetime of a wireless sensor network satisfy the promptness and security requirements of query processing applications in the presence of unreliable malicious nodes. We had applied the best design parameter settings at runtime in response to environment changes to prolong the system lifetime.

REFERENCES

[1] Hamid Al-Hamadi and Ing-Ray Chen"Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks," IEEE Trans. Network and service management, vol. 10, no. 2, June 2013.

[2] J. Deng, R. Han, and S. Mishra, "INSENS: intrusion-tolerant routing for wireless sensor networks," *Computer Commun.*, vol. 29, no. 2, pp.216–230, 2006.

[3] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE Trans. Mobile Comput.*, vol. 9, no. 7, pp. 941–954, 2010.

[4] F. Bao, I. R. Chen, M. Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 2, pp. 161–183, 2012.

[5] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Commun. Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28,2008.

[6] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem,"*ACM Trans. Programming Languages Syst.*, vol. 4, no. 3, pp.382–401, 1982.

[7] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," *J. Netw. Comput. Appl.*, vol. 33, no. 4, pp. 422–432, 2010.

[8] J. Deng, R. Han, and S. Mishra, "INSENS: intrusion-tolerant routing for wireless sensor networks," *Computer Commun.*, vol. 29, no. 2, pp.216–230, 2006.

[9] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing geographic routing in wireless sensor networks," in *Proc. 2006 Cyber Security Conf. Inf. Assurance*.

[10] W. Lou and Y. Kwon, "H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 55, no. 4, pp. 1320–1330, 2006.

[11] Y. X. Jiang and B. H. Zhao, "A secure routing protocol with malicious nodes detecting and diagnosing mechanism for wireless sensor networks," in *Proc. 2007 IEEE Asia-Pacific Service Comput. Conf.*, pp. 49–55.

[12] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and contermeasures," in *Proc*.