International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

To Enhance Lifetime of WSN Using Multi-Hop Routing and Trust-Based Intrusion Detection

Sanghavi Parkhi[1], Hemlata Dakhore[2]

[1]M. Tech Student, Department of CSE, G.H Raisoni Institute Of Engineering & Technology, Nagpur, India

[2]Assistant Professor, Department of CSE, G.H Raisoni Institute Of Engg & Tech, Nagpur, India

Abstract: ***In this paper, we will propose redundancy management of heterogeneous wireless sensor networks (HWSNs), using multihop routing to answer user queries in the existence of unreliable and malicious nodes. The key concept behind of our redundancy management is to exploit the balancing between energy consumption vs. timeliness, and security to increase the system useful lifetime. We will use an algorithm for Redundancy Management for identifying the best redundancy level to apply to multihop routing for intrusion tolerance, to increase the query success probability and system lifetime. Then we will use a voting-based distributed intrusion detection algorithm to detect and evict malicious nodes in a HWSN. We will develop a new probability model to analyze the best redundancy level in terms of path redundancy and source redundancy, and also the best intrusion detection in terms of the number of voters under which the lifetime of a HWSN is increased. We will then apply the analysis results obtained to the design of a particular redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes, to increase the HWSN lifetime. A prototype implementation in the ns2click simulator will be used to demonstrate malicious attacks launched by intruder nodes .***

Keywords: Wireless sensor networks, multi-hop routing, timeliness, security, energy conservation, Trust-Based Intrusion Detection.

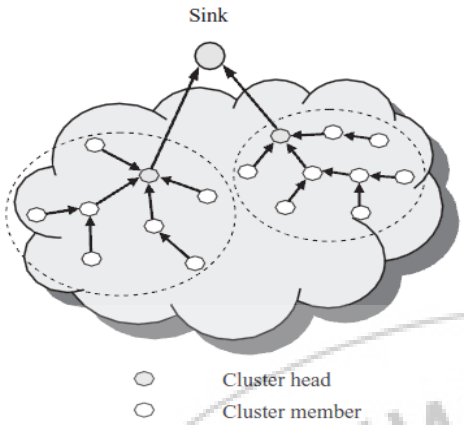
1. Introduction

Wireless sensor networks (WSNs) are very rapidly emerging as new area for various research. Applications of WSNs are numerous and growing rapidly from indoor deployment scenarios 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 which are in existence and used for monitoring and recording the physical conditions of the environment. The various monitoring types include Habitat Monitoring, Hazard Monitoring and Disaster Monitoring etc. Many wireless sensor networks (WSNs) are deployed in an environment which is unattendent and their recovering of energy is difficult even sometimes it is impossible. Hence, It should satisfy the timeliness, 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. timeliness 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(CH's) and Sensor Nodes(SN) connected in a network. Which uses homogeneous nodes which rotate among themselves in the roles of cluster heads. In heterogeneous WSN (HWSN) environments CH 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 timeliness and may also the complication if any malicious nodes are detected and the path will be broken. 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 to using multihop routing to tolerate insider attacks. These studies, however, largely ignored the balancing between QoS gain vs. energy consumption which can unfavourably shorten the system lifetime.

Multi-Hop routing is considered as an effective mechanism for fault and intrusion tolerance to improve data delivery in Wireless Sensor network. In multi-hop wireless networks, communication between two end nodes is carried out by using number of intermediate nodes which are used to send information from one end point to another. The basic idea behind it is that the probability of at least one path reaching the sink node or base station s as we have more paths doing data delivery.

Another approach which we will approve in this paper is the use local host-based IDS for energy conservation (in which SNs will monitoring neighbor SNs and CHs will monitoring neighbor CHs only), coupled with voting. Energy efficiency will be achieved by applying the optimal detection interval to perform IDS functions. Our solution will consider the optimal IDS detection interval that can best balance intrusion accuracy vs. energy consumption, so as to the system lifetime.



A HWSN will include sensors of different capabilities. We will consider sensors of two types : CHs (Cluster Heads)and SNs(Sensor Nodes). Any communication between more than two nodes will be done using multihop routing. Due to limited energy, a packet is sent hop by hop without making use of acknowledgment or retransmission. Queries can be anywhere in the HWSN through a nearby CH. A Cluster Head(CH) which takes a query to process is called a query processing center (PC). We will assume that, each query will have a strict timeliness requirement (T_{req}). The query must be delivered within T_{req} seconds; otherwise, the query will be failed.

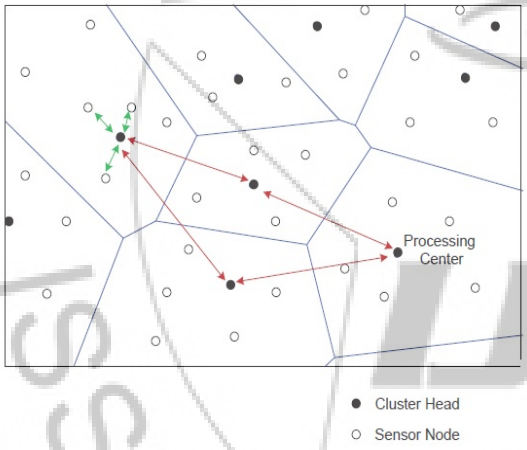


Figure 1: Source and path redundancy for a heterogeneous WSN

Redundancy management of multipath routing for intrusion tolerance will be achieved through two forms of redundancy: (a) source redundancy by which number of SNs per cluster in response to a query senses physical phenomenon in the same feature zone are used to forward sensing data to their CH (referred to as the source CH); (b) path redundancy by which, number of paths from a source CH to the sink are used to transfer packets from the source CH to the PC(Processing Center) through intermediate CHs. As part of clustering, a CH will know the locations of sensor nodes present within its cluster, and vice versa. A CH also knows the location of neighbor CHs along the direction towards the processing center.

For detecting compromised nodes, every node will run a simple *host IDS* to assess its neighbors. That is, each node will monitor its neighbor nodes only. Each node will make use of a set of anomaly detection rules. If the count will exceed a system-defined threshold value, a neighbor node that will be monitored will be considered as compromised.

2. Literature Survey

Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks

IN this paper, Hamid Al-Hamadi and Ing-Ray Chen, Member, IEEE had illustrated detail review of redundancy management of heterogeneous wireless sensor networks (HWSNs), which is used for utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. They had formulated the tradeoff as an 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.

2.1 Redundancy Management

Redundancy management of multipath routing for intrusion tolerance was achieved through two forms of redundancy:

a) Source redundancy by which SNs sensing a physical phenomenon in the same feature zone are used to forward
sensing data to their CH
b) Path redundancy by which paths were used to relay packets from the source CH to the PC through intermediate CHs.

2.2 Intrusion Tolerance

The algorithm dynamic redundancy management of multipath routing was used to describe the CH and SN execution protocols, respectively, for managing multipath routing for intrusion tolerance to increase the system lifetime. They were used to specify control actions taken by individual SNs and CHs in response to dynamically changing environments.

The various design parameters in terms of optimal T_{IDS}, m, m_s, and m_p were determined at static design time and pre-stored in a table over perceivable ranges of input parameter values. The action that was performed by a CH upon a T_D timer event includes (a) adjusting CH radio range to maintain CH connectivity ; (b)determining T_{IDS}, m, m_s, and m_p based on the sensed environmental conditions at runtime; and (c)notifying SNs within the cluster of the new T_{IDS} and m settings.

2.3 MTTF Calculation

In this ,m_p (path redundancy), m_s (source redundancy), m (the number of voters for intrusion detection) and T_{IDS}(the

intrusion detection interval) were taken as design parameters whose values were identified to increase MTTF i.e., lifetime of HWSN , when a set of input parameter values charactering the operational and environmental conditions were given. They had computed MTTF as the possibility weighted average of the number of queries the system can handle without experiencing any deadline, transmission, or security failure. More specifically, the MTTF is computed by:

$$MTTF = \sum_{i=1}^{N_q-1} i \left(\prod_{j=1}^{i} R_q(t_{Q,j}) \right) (1 - R_q(t_{Q,i+1})) + N_q \prod_{j=1}^{N_q} R_q(t_{Q,j})$$

where, *Rq(t)* was the Probability that a query reply at time *t* is delivered successfully by the deadline and *Nq was used as* Maximum number of queries before energy exhaustion, In First term i to j=1 Rq(tQ,j)was used to define the probability of the system being able to successfully execute *i* consecutive queries but failing the *i* + 1th query. In the second term the best case in which all queries will be processed successfully without experiencing any failure for which the system will have the longest lifetime span.

3. INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks

In this paper , Jing Deng, Richard Han, Shivakant Mishra had illustrated in detail review of an INtrusion-tolerant routing protocol for wireless SEnsor Networks (INSENS) is been described. INSENS is used to constructs 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 intrusions 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.

3.1 INSENS Protocol Design Principles

INSENS's design is based on three principles:

1) To Exploit redundancy to tolerate intrusions without any need for detecting the node(s) where intrusions have occurred. INSENS operates correctly in the presence of undetected intruders.
2) To Perform all heavy-duty computations at the base station(s), and minimize the role of sensor nodes in building routing tables, or dealing with security and intrusion-tolerance issues.
3) (iii)To Limit the scope of damage done by undetected intruders by limiting flooding and using appropriate authentication mechanisms. It uses symmetric-key cryptography to implement these mechanisms.

3.2 Route Discovery

Route discovery establish the topology of the sensor network and builds appropriate forwarding tables at various nodes. Route discovery is performed in three rounds. In the first round, the base station floods i.e, limited flooding, a request message was send to all the reachable sensor nodes in the network. In the second round, sensor nodes send their i.e, local, topology information using a feedback message to the base station. In the third round, the base station computes the forwarding tables for each sensor node based on the information received in the second round and sends them to the respective nodes by using a routing update message.

3.3 Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes

In this paper,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 “shares”: purely random propagation (PRP), directed random propagation (DRP), non-repetitive random propagation (NRRP), and multicast tree-assisted random propagation (MTRP).

3.3.1 Purely Random Propagation

In PRP, information which was shared, were propagated based on one-hop neighborhood information. Specifically, a sensor node was used to maintain a neighbor list, which contains the ideas of all the nodes that are within its receiving range. When a source node wants to send information shared to the sink, it used to include a TTL of initial value *N* in each share.

3.3.2 Non-repetitive Random Propagation:

NRRP was based on PRP, but it had improved propagation efficiency by recording all the nodes that the propagation had traversed till the time. Specifically, NRRP used to add a “node-in-route” (NIR) field to the header of each share. Initially, this field was empty. Starting from the source node, whenever a node transfers the share to the next hop, the id of the up-stream node was attach to the share’s NIR field.

3.3.3 Directed Random Propagation

DRP used two-hop neighborhood information. Specifically, DRP used to add a “last-hop neighbor list” (LHNL) field to the header of each share. Before a share was propagated to the next node, the relaying node used to first replaces the old content in the LHNL field of the share by its neighbor list.

3.3.4 Multicast Tree-assisted Random Propagation

The aim of MTRP was to actively improve the energy efficiency of random propagation while preserving the depressiveness of DRP. MTRP involved the directionality in its propagation process without needing location information. Specifically, after the arrangement of the WSN, MTRP requires that the sink constructs a multicast tree from itself to every node in the network.

3.3.5 Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection

In this paper, 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.

3.3.6 Hierarchical Trust Management Protocol

Their Hierarchical trust management protocol used to maintain two levels of trust: *SN-level* trust and *CH-level* trust. Each SN evaluates other SNs in the same cluster while each CH evaluates other CHs and SNs in its cluster. The peer-to-peer trust evaluation was periodically modified based on either *direct* observations or *indirect* observations. When two nodes are BAO neighbors within radio range, they evaluate each other based on direct observations via snooping or overhearing. Each SN sends its trust evaluation results toward other SNs in the same cluster to its CH.

4. Conclusion

In this paper, we will performed a balance analysis of energy consumption vs. QoS timeliness, and security for redundancy management of clustered heterogeneous wireless sensor networks (HWSN) by utilizing multipath routing to answer user queries. We will develop a probability model to analyze the best redundancy level in terms of both path redundancy (m_P) and source redundancy (m_S), as well as the best intrusion detection settings in terms of the number of voters (m) and the intrusion invocation interval (T_{IDS}) under which the lifetime of a heterogeneous wireless sensor network will be d while satisfying the timeliness and security requirements of query processing applications in the presence of unreliable malicious nodes and Finally we will show an graphical analysis of the Comparisons between the Voting Based algorithm and the new algorithm by using a network simulator.

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.