

Lifetime Maximization in Heterogeneous wireless Sensor Networks using Multipath Routing Technique

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- In wireless sensor Networks security is one of the important problems we are facing. To provide redundancy management for heterogeneous wireless sensor networks (HWSNs) utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. In this paper use a Multipath Routing, it is the routing technique of using multiple alternative paths through the network. The objective of redundancy management of multipath routing minimizes the energy loss and gain in reliability, timeliness and security to maximize the system lifetime. Here a voting based intrusion detection algorithm used to detect and evict malicious nodes. We plan to explore more extensive malicious attacks for packet dropping and bad mouthing attacks with implications to energy reliability and security, and investigate Intrusion detection and multipath routing based acceptance protocols to react to these attacks.

Index Terms- Heterogeneous wireless sensor networks, intrusion detection, multipath routing, security.

I. INTRODUCTION

Wireless sensor networks (WSN) is a growing technology which is offering solution for many Application areas such as health care, military, industry and also environmental conditions like temperature, sound, gas, pressure. SNs are used for sensing the environments are used to read the sensing information and transmit to base station and also used for monitoring purposes Sensor node is a tiny device includes five basic components 1)controller 2)communication devices 3)sensors/actuators 4) memory 5) power supply. These sensor networks are used for many critical applications where security is also critical and energy replacement is difficult if not impossible. So it is important satisfy application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to extend the system useful period of time. The trade of between energy consumption and gain in reliability gain with goal maximize the WSN system lifetime has been well explored in the literature. However, no prior work exits to consider the trade-off within the presence of malicious attackers.

Naturally, grouping of sensor nodes in to clusters has been widely used in research community to satisfy scalability and generally achieve high energy efficiency and prolong the network lifetime in large-scale WSN environment. In the hierarchical network structure each cluster has a leader which

Also called as cluster Head (CH) and usually performs the special tasks referred above (fusion and aggregation), and several common sensor nodes (SN) as members. The cluster formation process eventually leads to a two-level hierarchy where the CH nodes form the higher level and the cluster-member nodes form the lower level. The sensor nodes periodically transmit their data to the corresponding CH nodes.

On the other hand, security in WSNs is an important issue, especially if they have mission-critical tasks. For instance, a confidential patient health record should not be released to third parties in a health care application. Securing WSNs is critically important in tactical (military) applications where a security gap in the network would cause casualties of the friendly forces in a battlefield. Security attacks against WSNs are categorized into two main branches: Active and Passive. In passive attacks, attackers are typically camouflaged (hidden) and either tap the communication link to collect data; or destroy the functioning elements of the network. Passive attacks can be grouped into eavesdropping, node malfunctioning, node tampering/ destruction and traffic analysis types. In active attacks, an adversary actually affects the operations in the attacked network. This effect may be the objective of the attack and can be detected. For example, the networking services may be degraded or terminated as a result of these attacks. Active attacks can be grouped into Denial-of-Service, black hole, wormhole, sinkhole, etc.), flooding and Sybil types.

Intrusion is an unauthorized (unwanted) activity in a network that is either achieved passively (e.g., information gathering, eavesdropping) or actively (e.g., harmful packet forwarding, packet dropping, hole attacks). In a security system, if the first line of defense, "Intrusion Prevention," does not prevent intrusions, then the second line of defense, "Intrusion Detection," comes into play. It is the detection of any suspicious behavior in a network performed by the network members. In any security plan, Intrusion Detection Systems (IDSs) provide some or all of the following information to the other supportive systems: identification of the intruder, location of the intruder (e.g., single node or regional), time (e.g., date) of the intrusion, intrusion activity (e.g., active or passive), intrusion type (e.g., attacks such as worm hole, black hole, sink hole, selective forwarding, etc.), layer where the intrusion occurs (e.g., physical, data link, network). This information would be very helpful in mitigating (i.e., third line of defense) and remedying the result attacks, since very specific information regarding the intruder is obtained. Therefore, intrusion detection systems are very important for network security.

Intrusions over the web have become additional dynamic and complicated. Intrusion detection Systems determines intrusions by scrutiny noticeable behavior against suspicious patterns. There are two types of intrusion detection systems.

Network based IDS: these types of IDS are strategically positioned in a network to detect any attack on the hosts of that network. To capture all the data passing through the network, you need to position your IDS at the entry and exit point of data from your network to the outside world. You can also position some IDS near the strategic positions of your internal network, depending on the level of security needed in your network. Since a network based IDS need to monitor all the data passing through the network, it needs to be very fast to analyze the traffic and should drop as little traffic as possible.

Host based IDS: they are installed in a host and they can monitor traffics that are originating and coming to those particular hosts only. If there are attacks in any other part of the network, they will not be detected by the host based IDS.. Apart from monitoring incoming and outgoing traffic, a host based IDS can also analysis the file system of a host, users' logon activities, running processes, data integrity etc.

The intrusion detection can be analyzed according to the capability of sensors in terms of the transmission range and sensing range. In a heterogeneous WSN some sensors have a large power to achieve a longer transmission range and large sensing range. Recent studies [2], [3] demonstrated that using heterogeneous nodes can enhance performance and prolong the system lifetime. In the latter case, nodes with superior resources serve as CHs performing computationally intensive tasks while inexpensive less capable SNs are utilized mainly for sensing the environment. Thus, the heterogeneous WSN increases the detection probability for a given intrusion detection system. It is commonly believed in the research community that clustering [4], is an effective solution for achieving scalability, energy conservation, and reliability. Therefore the cluster based heterogeneous WSN can further improves the performance of the network.

Multipath routing is taken into account a good mechanism for fault and intrusion tolerance to boost data delivery in WSNs. The fundamental plan is that the chance of a minimum of one path reaching sink node or base station will increase as we've additional methods doing data delivery. HWSN includes sensors of various capabilities. We tend to contemplate two sorts of sensors: CHs and SNs. CHs square measure superior in energy and machine resources. Most prior research focused on using multipath routing to improve reliability [5], [6], and tolerate inside attacks [7]. However, these studies largely ignored energy consumption which can adversely shorten the system lifetime.

Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities and produces reports to base station. Intrusion Detection and prevention System (IDPS) primarily focused on identifying possible incidents, logging information about them and reporting attempts. And also address the energy consumption and QoS gain in reliability, timeliness, and security with the goal to maximize the lifetime of clustered HWSN while satisfying application requirements in the context of multipath

routing. More specifically, to analyze the optimal amount of redundancy through which data are routed to a remote sink or base station in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime.

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 a node is considered misbehaving to optimize the application performance in false alarm probability.

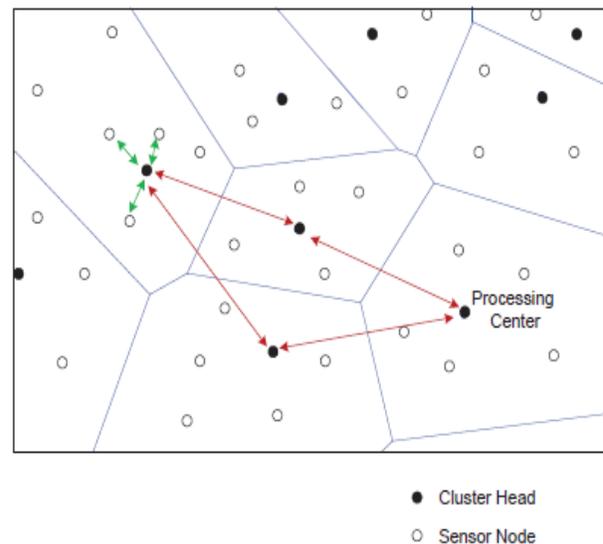


Figure.1 Source and path redundancy for a HWSN

II REASERCH ELABORATIONS

Over the past few years, many protocols exploring the energy consumption and QoS gain particularly in reliability in Heterogeneous Wireless Sensors (HWSNs) have been proposed.

In [5], the optimal communication range and communication mode were to maximize the HWSN lifetime. In [6], the authors devised intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network life time. They considered a HWSN with CH nodes having larger energy and processing capabilities compare to SNs in the network. The solution is drawn as an optimization problem to balance energy consumption across all nodes within the network along with their roles. In either work [7], [8], no consideration was taken in to account about the existence malicious nodes in the network. Relative to [8] the proposed work considers the presence of malicious nodes and explores the tradeoff in energy consumption and QoS gain in both security and reliability to maximize the system lifetime. In the context of secure multipath routing for Intrusion tolerance, [9] provides excellent survey in this topic. In [15] the authors considered a multipath routing protocol to tolerate black hole and selective forwarding attacks. The basic idea is to use overhearing to avoid sending packets to malicious nodes. Our work also uses multipath routing to tolerate intrusions. However, we specifically consider energy being consumed for intrusion detection, and both CHs and SNs can be compromised for lifetime maximization.

Over the past few years, numerous protocols have been proposed to detect intrusion in WSNs. [7, 11] provide excellent surveys of the subject. In [10], a decentralized rule-based intrusion detection system is proposed by which monitor nodes are responsible for monitoring neighboring nodes. The monitor nodes apply predefined rules to collect messages and raise alarms if the number of failures exceeds a threshold value. Our host IDS essentially follows this strategy, with the flaws of the host IDS characterized by a false positive probability (H_{pfp}) and a false negative probability (H_{pfn}). In [10], however, no consideration is given about bad-mouthing attacks by compromised monitor nodes themselves, so if a monitor node is malicious, it can quickly infect others. In [8], a collaborative approach is proposed for intrusion detection where the decision is based on a majority voting of monitoring nodes. Their work, however, does not consider energy consumption issues associated with a distributed IDS, nor the issue of maximizing the WSN lifetime while satisfying QoS requirements in security, reliability and timeliness. Our voting-based IDS approach extends from [9] with considerations given to the tradeoff between energy loss vs. security and reliability gain due to employment of the voting-based IDS with the goal to prolong the system lifetime.

Redundancy management of multipath routing for intrusion tolerance is achieved through two forms of redundancy: (a) source redundancy by which ms SNs sensing a 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 mp paths are used to relay packets from the source CH to the PC through intermediate CHs. Fig. 1 shows a scenario with a source redundancy of 3 ($ms = 3$) and a path redundancy of 2 ($mp = 2$). It has been reported that the number of edge-disjoint paths between nodes is equal to the average node degree with a very high probability. Therefore, when the density is sufficiently high such that the average number of one-hop neighbors is sufficiently larger than mp and ms , we can

effectively result in mp redundant paths for path redundancy and ms distinct paths from ms sensors for source redundancy.

In general there are two approaches by which energy efficient IDS can be implemented in WSNs. One approach especially applicable to flat WSNs is for an intermediate node to feedback maliciousness and energy status of its neighbor nodes to the sender node (e.g., the source or sink node) who can then utilize the knowledge to route packets to avoid nodes with unacceptable maliciousness or energy status [17, 24]. Another approach which we adopt in this paper is to use local host-based IDS for energy conservation (with SNs monitoring neighbor SNs and CHs monitoring neighbor CHs only), coupled with voting to cope with node collusion for implementing IDS functions. Energy efficiency is achieved by applying the optimal detection interval to perform IDS functions. Our solution considers the optimal IDS detection interval that can best balance intrusion accuracy vs. energy consumption due to intrusion detection activities, so as to maximize the system lifetime.

To detect compromised nodes, every node runs a simple *host IDS* to assess its neighbors. Our host IDS is light-weight to conserve energy. It is also generic and does not rely on the feedback mechanism tied in with a specific routing protocol (e.g., MDMP for WSNs [17] or AODV for MANETs [18]). It is based on local monitoring. That is, each node monitors its neighbor nodes only. Each node uses a set of anomaly detection rules such as a high discrepancy in the sensor reading or recommendation has been experienced, a packet is not forwarded as requested, as well as interval, retransmission, repetition, and delay rules as in [10, 31-33]. If the count exceeds a system-defined threshold, a neighbor node that is being monitored is considered compromised.

To remove malicious nodes from the system, a voting based distributed IDS is applied periodically in every TIDS 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.

Compared with existing works cited above, our work is distinct in that we consider redundancy management for both intrusion/fault tolerance through multipath routing and intrusion detection through voting-based IDS design to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes.

The proposed research work extends from [1] with considerations given to explore more extensive malicious attacks, each with different implications to energy, security and reliability, and also investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks. In addition to this the proposed work also consider smart and insidious attackers which can perform more targeted attacks,

capture certain nodes with high probability, alternate between benign and malicious behavior and concatenate with other attackers to avoid intrusion detection. Also to investigate the use of trust/reputation management [12], [13] to strengthen intrusion detection through “weighted voting” [14] leveraging knowledge of trust/reputation of neighbor nodes. Using weighted voting scheme in intrusion detection system (IDS) would considerably reduce the false positives (FPs) and false negatives (FNs) ratio. The accuracy is the percentage of whole traces that are determined accurately, while the efficiency indicates that the voting algorithm performs better on reducing both FP and FN ratios. The weighted voting scheme achieved efficiency. The propose work also tackle the “what paths to use” problem in multipath routing decision making for intrusion tolerance in WSNs, so to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes.

Light weight detection system is used to detect malicious nodes in the network. The objective of Light weight intrusion detection System can easily be deployed in any node of a network, with minimal disruptions to operations. Easily be configured by system administrators who need to implement a specific security solution in a short amount of time. It is small, powerful and flexible enough to be used as permanent elements of the network security infrastructure .In the Detection Algorithm no malicious nodes appear during the initial stage of sensor node deployment. SNs maintain two databases namely: 1) Malicious nodes and 2) Neighbor knowledge in the neighbor knowledge, broadcasting protocols are used to reduce the number of transmissions. And to detect the warm hole attacks in WSNs. In the malicious nodes, malicious counter have suspicious node stored in a CH crosses a threshold x means CHs creates and propagate a new rule to each and every SNs node in cluster. Then SNs update a new rule and add entry to its malicious database and malicious node is isolated from cluster and not involved in communication in the network.

III CONCLUSION

In this paper we performed a tradeoff analysis of energy consumption vs. QoS gain in reliability, timeliness, and security for redundancy management of clustered heterogeneous wireless sensing element networks utilizing multipath routing to answer user queries. The trust/reputation management system is also used to strengthen intrusion detection through weighted voting based mechanisms and finally light weight intrusion detection method is used to detect malicious nodes in the networks. For future work more efficient trust based system are used for to enhance the performance of the system.

IV 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] Mohamed Mubarak T, Syed Abdul Sattar, G.Appa Rao, Sajitha M, “Intrusion detection: An Energy efficient approach in Heterogeneous

- WSN,” in *proc.2011 IEEE International Conference on Emerging Trends in Electrical and Computer Technology*.
- [3] X. Du and F. Lin, “Improving routing in sensor networks with heterogeneous sensor nodes,” in *Proc. 2005 IEEE Veh. Technol. Conf.*, pp 2528-2532.
- [4] S. Bandyopadhyay and E. J. Coyle, “An energy efficient hierarchical clustering algorithm for wireless sensor networks,” in *Proc. 2003 Conf. IEEE Computer Commun.*, pp. 1713–1723.
- [5] E. Felemban, L. Chang-Gun, and E. Ekici, “MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks,” *IEEE Trans. Mobile Computing.*, vol. 5, no. 6, pp. 738–754, 2006.
- [6] I. R. Chen, A. P. Speer, and M. Eltoweissy, “Adaptive fault-tolerant QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks,” *IEEE Trans. Dependable Secure Computing*, vol. 8, no. 2, pp. 161–176,
- [7] 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.
- [8] H. Su and X. Zhang, “Network lifetime optimization for heterogeneous sensor networks with mixed communication modes,” in *Proc. 2007 IEEE Wireless Commun. Netw. Conf.*, pp. 3158–3163.
- [9] I. Slama, B. Jouaber, and D. Zeghlache, “Optimal power management scheme for heterogeneous wireless sensor networks: lifetime maximization under QoS and energy constraints,” in *Proc. 2007 IEEE Int. Conf. Netw. Services*, pp. 69–69.
- [10] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, “Securing geographic routing in wireless sensor networks,” in *Proc. 2006 IEEE Cyber Security Conf. Inf. Assurance*.
- [11] 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.
- [12] 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.
- [13] C. J. Fung, Z. Jie, I. Aib, and R. Boutaba, “Dirichlet-based trust management for effective collaborative intrusion detection networks,” *IEEE Trans. Netw. Service Manage.*, vol. 8, no. 2, pp. 79–91, 2011.
- [14] Ahmed Alahmadi and Ben Soh, “A Hybrid History Based Weighted Voting Algorithm for Ultra-Critical Systems,” in *Proc. 2012 IEEE Int. Conf. Symposium on Communications and Information Technologies (ISCIIT)*, pp. 4673-1157.

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.