Maximizing the Network Lifetime in Heterogeneous WSN through Multipath Routing

Kavitha Kengal
M.Tech, Dept, of CSE,
AMC Engineering College,
Bangalore-560083, India
Kavitha.kengal@gmail.com

Doddegowda B J
Associate Professor, Dept, of CSE,
AMC Engineering College,
Bangalore-560083, India
bjdgowda10@gmail.com

Abstract **- In redundancy management of heterogeneous wireless sensor networks (HWSNs), it utilizes multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of redundancy management is to exploit the trade-off between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. Furthermore, it considers the optimization problem for the case in which a voting - based distributed intrusion detection algorithm is applied to detect and evict malicious nodes in a HWSN. Here it uses a novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy. After that it applies the analysis results obtained to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes to maximize the HWSN lifetime.**

Keywords — Heterogeneous wireless sensor networks, multipath routing, intrusion detection, reliability, security, energy conservation.

I. INTRODUCTION

Wireless Sensor Network (WSNs) consists of thousands of tiny nodes having the capability of sensing, computation, and wireless communications. Wireless sensor nodes that senses the environment to get information on how the fire spreads. They form a wireless network to communicate their information. The information about where the fire is and how it is spreading is collected by the fire fighters and helps them take decisions on the best way to fight the fire.

Wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations.

The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Many routing, power management, and data dissemination protocols have been specifically designed for WSNs where energy consumption is an essential design issues. Since wireless sensor network protocols are application specific, so the focus has been given to the routing protocols that might differ depending on the application and network architecture. The study of various routing protocols for sensor networks presents a classification for the various approaches pursued. The three main categories explored are data centric, hierarchical and location-based. Each of the routing schemes and algorithms has the common objective of trying to get better throughput and to extend the lifetime of the sensor network.

Lot of existing intrusion Detection Systems (IDSs) examines the network packets individually within both the web server and the database system. However, there is very little work being performed on multi-tiered Anomaly Detection (AD) systems that generate the models of network behavior for both web and database network interactions.

In such multitier architectures, the back-end database server is often protected behind a firewall while the web servers are remotely accessible over the Internet. Unfortunately, though they are protected from direct remote attacks, the back-end systems are susceptible to attacks that use web requests as a means to exploit the back end. In order to protect multi-tiered web services, an efficient system called as Intrusion detection systems is needed to detect known attacks by matching misused traffic patterns or signatures. For the issue of intrusion tolerance through multipath routing, there are two major problems to solve: (1) How many paths to use and (2) what paths to use.

Proposed system develops a probability model to estimate the MTTF of a HWSN using multipath data forwarding to answer queries issued from a mobile user

roaming in the HWSN area. The basic idea of MTTF formulation is that, first deduce the maximum number of queries, *Nq* ,the system can possible handle before running into energy exhaustion for the best case in which all queries are processed successfully. The second term is for the best case in which all queries are processed successfully without experiencing any failure for which the system will have the longest lifetime span.

- Network Dynamics.
- Query Success Probability.
- Energy Consumption.

The objective of dynamic redundancy management is to dynamically identify and apply the best redundancy level in terms of path redundancy (*mp*) and source redundancy (*ms*), as well as the best intrusion detection settings in terms of the number of voters (*m*) and the intrusion invocation interval to maximize MTTF, in response to environment changes to input parameters in and SN/CH capture rate (λc). the algorithm for dynamic redundancy management of multipath routing is distributed in nature. CH(Cluster Head) and SN(Sensor Nodes) execution protocols, respectively, for managing multipath routing for intrusion tolerance to maximize the system lifetime.

A. Intrusion Detection System

An intrusion detection system (IDS) is an active process or device that analyzes system and network activity for unauthorized entry and/or malicious activity. The way that an IDS detects anomalies can vary widely; however, the ultimate aim of any IDS is to catch perpetrators in the act before they do real damage to resources. For the issue of intrusion tolerance through multipath routing, there are two major problems to solve: (1) how many paths to use and (2) what paths to use.

Here it first addresses that "how many paths to use" problem. Next it addresses "what paths to use" problem, this approach is distinct from existing work in that it does not consider specific routing protocols (e.g., MDMP for WSNS[5],[6]) nor the use of feedback information to solve the problem. Rather, for energy conservation, it employs a distributed light-weight IDS by which intrusion detection is performed only locally. Nodes that are identified compromised are removed from the HWSN.

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

B. Multipath Routing

It uses multiple paths in order to enhance network performance

- Fault tolerance
- Balance energy consumption
- Energy-efficient
- Reliability

In this routing protocol that uses the multiple paths rather than a single path in order to enhance the network performance. The fault tolerance (resilience) of a protocol is measured by the likelihood that an alternate path exists between a source and a destination when the primary path fails. This can be increased by maintaining multiple paths between the source and the destination at the expense of an increased energy consumption and track generation. These alternate paths are kept alive by sending periodic messages. Hence, network reliability can be increased at the expense of increased overhead of maintaining the alternate paths.

Here it uses an algorithm which will route data through a path whose nodes have the largest residual energy. The path is changed whenever a better path is discovered. The primary path will be used until its energy falls below the energy of the backup path at which the backup path is used. Using this approach, the nodes in the primary path will not deplete their energy resources through continual use of the same route, hence achieving longer life. However, the path switching cost was not quantified. It also explains the use of a set of sub-optimal paths occasionally to increase the lifetime of the network. These paths are chosen by means of a probability which depends on how low the energy consumption of each path is.

C. Contributions

- Managing redundancy in multipath routing.Using intrusion tolerance to detect the malicious nodes.
- Analyzing best redundancy level in terms of path redundancy and source redundancy.
- Maximizing heterogeneous WSN's useful lifetime in presence of malicious nodes.

II. RELATED WORK

Over the past few years, many protocols exploring the trade-off between energy consumption and QoS gain particularly in reliability in HWSNs have been proposed. The optimal communication range and communication mode were derived to maximize the HWSN lifetime. The authors devised intra-cluster scheduling and intercluster multi-hop routing schemes to maximize the network lifetime.

They considered a hierarchal HWSN with CH nodes having larger energy and processing capabilities than

normal SNs. The solution is formulated as an optimization problem to balance energy consumption across all nodes with their roles. In either work cited above, no consideration was given to the existence of malicious nodes.

The authors considered a two-tier HWSN with the objective of maximizing network lifetime while fulfilling power management and coverage objectives. They determined the optimal density ratio of the two tier's nodes to maximize the system lifetime. Relative work also considers heterogeneous nodes with different 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.

This 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 compared with existing works cited above, this 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.

In [3], the optimal communication range and communication mode were derived to maximize the HWSN lifetime.

In [7], the authors devised intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a hierarchal HWSN with CH nodes having larger energy and processing capabilities than normal WSNs.

The solution is formulated as an optimization problem to balance energy consumption across all nodes with their roles. In either work cited above, no consideration was given to the existence of malicious nodes.

In [8], the authors considered a two-tier HWSN with the objective of maximizing network lifetime while fulfilling power management and coverage objectives. They determined the optimal density ratio of the two tier's nodes to maximize the system lifetime. In the context of secure multipath routing for intrusion tolerance, [9] provides an excellent survey in this work. In [4] 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.

In [1], 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. This voting-based IDS approach extends from effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks [2] 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.

Now current work is distinct in that 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.

III. SYSTEM MODEL

A HWSN comprises sensors of different capabilities. We consider two types of sensors: CHs and SNs. CHs are superior to SNs in energy and computational resources. We use E_{INIT}^{CH} and E_{INIT}^{SN} to denote the initial energy levels of CHs and SNs respectively. While our approach can be applied to any shape of the operational area, for analytical tractability, we assume that the deployment area of the HWSN is of size *A2*. CHs and SNs are distributed in the operational area. To ensure coverage, we assume that CHs and SNs are deployed randomly and distributed according to homogeneous spatial Poisson processes with intensities λ_{CH} and λ_{SN}, respectively, with $\lambda_{CH} < \lambda_{SN}$. The radio ranges used by CH and SN transmission is denoted by r_{CH} and r_{SN}, respectively. The radio range and the transmission power of both CHs and SNs are dynamically adjusted throughout the system lifetime to maintain the connectivity between CHs and between SNs.

Any communication between two nodes with a distance greater than single hop radio range between them would require multi-hop routing. Due to limited energy, a packet is sent hop by hop without using acknowledgment or retransmission [10]. All sensors are subject to capture attacks, i.e., they are vulnerable to physical capture by the adversary after which their code is compromised and they become *inside* attackers. Since all sensors are randomly located in the operational area, the same capture rate applies to both CHs and SNs, and, as a result, the compromised nodes are also randomly distributed in the operation area. Due to limited resources, we assume that when a node is compromised, it only performs two most energy conserving attacks, namely, *bad-mouthing attacks* (recommending a good node as a bad node and a bad node as a good node) when serving as a recommender, and *packet dropping attacks* [11] when performing packet routing to disrupt the operation of the network..

Queries can be issued by a mobile user (while moving) and can be issued anywhere in the HWSN through a nearby CH. A CH which takes a query to process is called a query processing center (PC). Many mission critical applications, e.g., emergency rescue and military battlefield, have a deadline requirement. We assume that each query has a strict timeliness requirement (*Treq*).

The query must be delivered within *Treq* seconds; otherwise, the query fails.

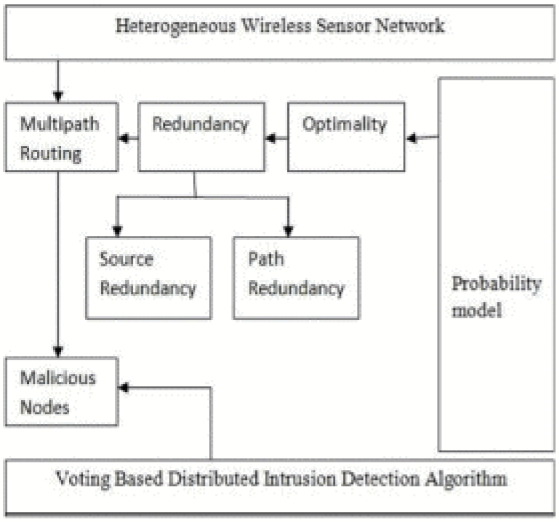

Figure1 Architectural Diagram

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 [26]. 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.

IV. ALGORITHM FOR DYNAMIC REDUNDANCY MANAGEMENT OF MULTIPATH ROUTING

The algorithms for dynamic redundancy management of multipath routing is distributed in nature. Algorithm 1 and 2 describes the CH and SN execution protocols, respectively, for managing multipath routing for intrusion tolerance to maximize the system lifetime. They specify control actions taken by individual SNs and CHs in response to dynamically changing environments.

Algorithm 1 *CH Execution for Dynamic Redundancy Management*

```
1:  CH Execution:
2:   Get next event
3:   if event is T_D timer then
4:        determine radio range to maintain CH connectivity
5:        determine optimal T_IDS, m, m_s, m_p by
            table lookup based on the current estimated
            density, CH radio range and compromise rate
6:        notify SNs within the cluster of the new
            optimal settings of T_IDS and m
7:   else if event is query arrival then
8:        trigger multipath routing using m_s and m_p
9:   else if event is T_clustering timer then
10:       perform clustering
11:  else if event is T_IDS timer then
12:       For each neighbor CH
13:            if selected as a voter then
14:                 execute voting based intrusion detection
15:  else // event is data packet arrival
16:       follow multipath routing protocol design to route
            the data packet
```

Algorithm 2 *SN Execution for Dynamic Redundancy Management*

```
1:  SN Execution:
2:   Get next event
3:   if event is T_D timer then
4:        determine radio range to maintain SN connectivity
            within a cluster
5:   else if event is control packet arrival from CH then
6:        Change the optimal settings of T_IDS, and m
7:   else if event is T_clustering timer then
8:        perform clustering
9:   else if event is T_IDS timer then
10:       For each neighbor SN
11:            if selected as a voter then
12:                 execute votingbased intrusion detection
13:  else // event is data packet arrival
14:       follow multipath routing protocol design to route
            the data packet
```

V. CONCLUSION

Trade-off analysis of energy consumption vs. QoS gain in reliability, timeliness, and security for redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries are performed.

A novel probability model was analyzed for the best redundancy level in terms of path redundancy (mp) and source redundancy (ms), as well as the best intrusion detection settings in terms of the number of voters (m) and the intrusion invocation interval under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security requirements of query

processing applications in the presence of unreliable wireless communication and malicious nodes.

Finally, analysis results to the design of a dynamic redundancy management algorithm is applied to identify and the best design parameter settings at runtime in response to environment changes to prolong the system lifetime.

VI. FUTURE WORK

For future work plans to explore more extensive malicious attacks in addition to packet dropping and bad mouthing attacks, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks.

Another direction is to consider smart and insidious attackers which can perform more targeted attacks, capture certain strategic nodes with higher probability, alternate between benign and malicious behavior and collude with other attackers to avoid intrusion detection. Further plan is to explore trust-based admission control to optimize application performance.

REFERENCES

[1] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," 13th European Wireless Conference, Paris,

[2] J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks," IEEE Trans. Rel., vol. 59, no. 1, pp. 231-241, 2010.

[3] H. Su and X. Zhang, "Network Lifetime Optimization for Heterogeneous Sensor Networks With Mixed Communication Modes," IEEE Wireless Communications and Networking Conference, 2007, pp. 3158-3163.

[4] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing Geographic Routing in Wireless Sensor Networks," 9th Annu. Cyber Security Conf. on Information Assurance, Albany, NY, USA, 2006.

[5] Y. Lan, L. Lei, and G. Fuxiang, " A multipath secure routing protocol based on malicious node detection," Chinese Control and Decision Conference, 2009, pp. 4323-4328.

[6] D. Somasundaram and R. Marimuthu, "A Multipath Reliable Routing fordetection and isolation of malicious nodes in MANET," International Conference on Computing, Communication and Networking, 2008, pp. 1-8.

[7] I. Slama, B. Jouaber, and D. Zeghlache, "Optimal Power management scheme for Heterogeneous Wireless Sensor Networks: Lifetime Maximization under QoS and Energy Constraints," Third International Conference on Networking and Services (ICNS) 2007, pp. 69-69

[8] R. Machado, N. Ansari, G. Wang, and S. Tekinay, "Adaptive density control in heterogeneous wireless sensor networks with and without power management," IET Communications, vol. 4, no. 7, pp. 758-767,2010

[9] 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. 941954, 2010.

[10] 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 Comput., vol. 5, no. 6, pp.738-754, 2006

[11] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," 1st IEEE Int. Workshop on Sensor Network Protocols and Applications, 2003, pp. 113-127.