INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

MULTIPATH SECURE ROUTING FOR INTRUSION TOLERANCE IN HETEROGENOUS WIRELESS SENSOR NETWORKS

Shaik.Tanveer Sultana[1], S.Rajiya Sulthana [2]

[1]Master's student, Department of CSE, Bharath college of engineering and technology for women,kadapa.
[2]Assistant Professor, Department of CSE, Bharath college of engineering and technology for women,kadapa.
Tanu.jb5816@gamil.com[1]
Rajiyasulthana21@gmail.com[2]

Abstract:

Aim of project is to develop a novel probability model to analyze best redundancy level In terms of path redundancy, source redundancy and best IDs. The contribution of project is to decide "how many paths to use and which path to use" in order to tolerate residual compromised node that survive our IDs to increase the life time of diverse wireless sensor networks. This is especially a critical issue in military or mission-critical WSN applications. Sensor nodes (SNs) close to the base station (BS) are more critical in gathering and routing sensing data. In the literature, various schemes have been designed for preserving critical SNs from energy exhaustion so as to prolong the system lifetime maximization; however, how to counter selective capture. We propose and analyze an adaptive network management algorithm with 3 countermeasures to counter selective capture: (1) optimal communication range and mode adjustment; (2) intra-clustering scheduling and inter-cluster multihop routing scheme; and (3) voting based intrusion detection. We develop a probability model to reveal the tradeoff between energy consumption vs. reliability and security gain with the goal to maximize the lifetime of a query-based WSN.

Keywords: heterogeneous wireless sensor networks, selective capture multipath Routing, lifetime maximization, intrusion detection, reliability, security, energy Conservation**.**

I. Introduction

Many wireless sensor networks (WSNs) are deployed in neglected environment in which energy replenishment is difficult but not impossible. Due to limited resources, a WSN should satisfy the application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to continuous usage of system lifetime. The tradeoffs between *energy* consumption Vs *reliability* gain with the goal to maximize the WSN system lifetime. A critical issue in military, business WSN applications. Sensor nodes (SNs) close to the base station (BS) are more critical in gathering and routing sensing data. In the literature, various schemes have been designed for preserving critical SNs from energy exhaustion so as to prolong the system lifetime; however, how to

Vol.2 Issue 8, Pg.: 136-142
August 2014

counter selective capture. We consider this optimization problem for the case in which a voting based distributed intrusion detection algorithm is applied to remove malicious nodes from the HWSN. 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. We analyze the optimal amount of redundancy for multipath routing and the best intrusion detection settings for detection strength under which the lifetime of a query-based WSN is maximized in the presence of selective capture.

II. Related Work

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 [2]. 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.* when performing packet routing to disrupt the operation of the network. Using homogeneous nodes which rotate among themselves in the roles of cluster heads (CHs) and sensor nodes (SNs) leveraging CH election protocols such as HEED [12] for lifetime maximization has been considered [2], [3]. In the optimal communication range and communication mode were derived to maximize the diverse WSN lifetime. In intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime.

In [4], the authors considered a two-tier diverse WSN 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. Our work considers the presence of malicious nodes and explores the tradeoff between energy consumption vs. QoS gain in both security and reliability to maximize the system lifetime.

III. Proposed System

Faith Based Neighbor Weighted Voting Scheme to strengthen intrusion detection in WSN is evaluate the dynamic radio range of neighbor nodes. Identification of multi source multipath routing for intrusion tolerance at higher levels. Neighbor Weighted Voting algorithm provides Faith weight of each neighbor sensor node. Weight threshold is evaluated for marking the sensor node as normal node and malicious node.

Discard the communication of internal malicious node by identifying lower weight votes of corresponding sensor node. The best number of voters and the intrusion invocation interval used for intrusion detection under which the lifetime of a WSN is maximized in the presence of selective capture which turns nodes into malicious nodes capable of performing packet dropping attacks and bad-mouthing attacks.

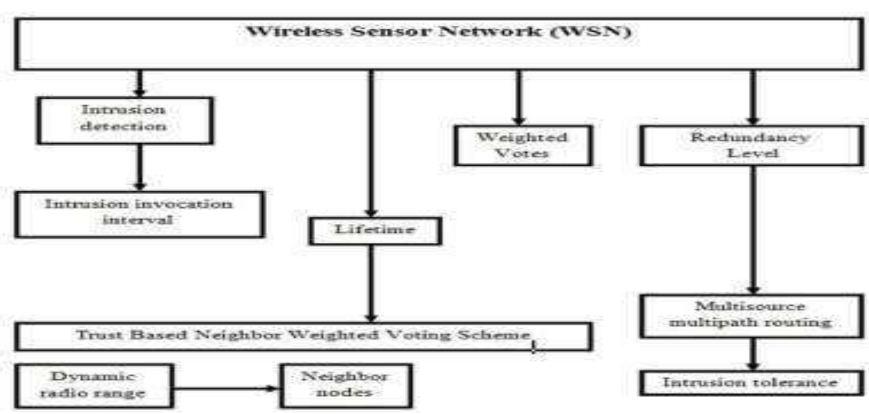


Fig.1. Architecture Diagram of Faith Based Neighbor Weighted Voting Scheme for Intrusion Tolerance in WSN

Vol.2 Issue 8, Pg.: 136-142
August 2014

Wireless Sensor Network

WSN comprises sensors of different capabilities types of sensors are Cluster Heads (CHs) and Sensor Nodes (SNs).CHs are superior to SNs in energy and computational resources, denote the initial energy levels of CHs and SNs, and applied to any shape of the operational area.

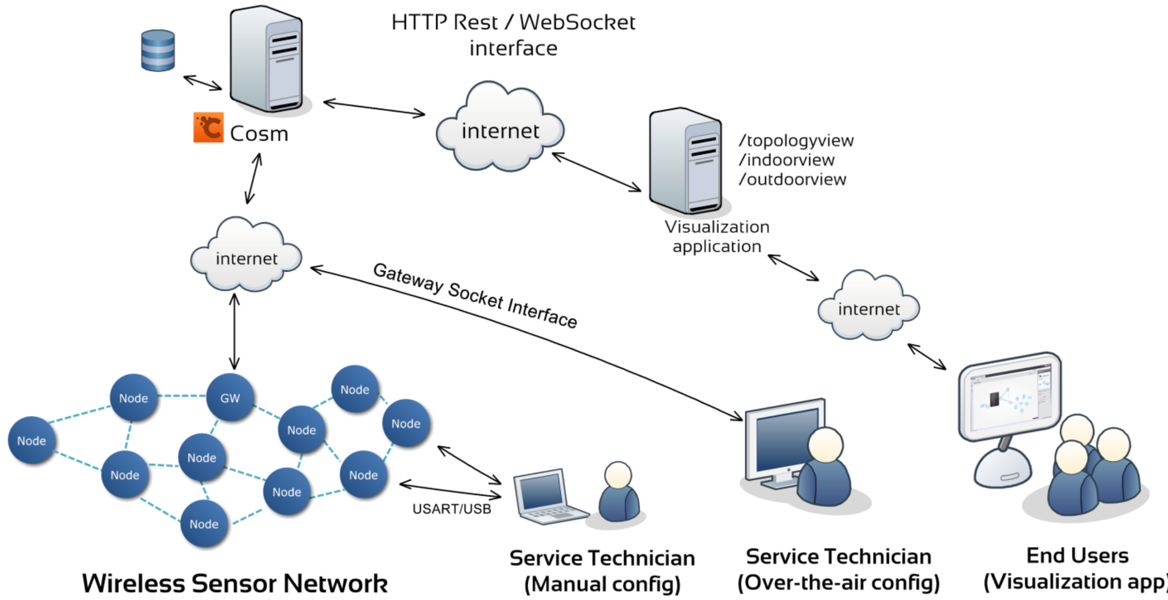
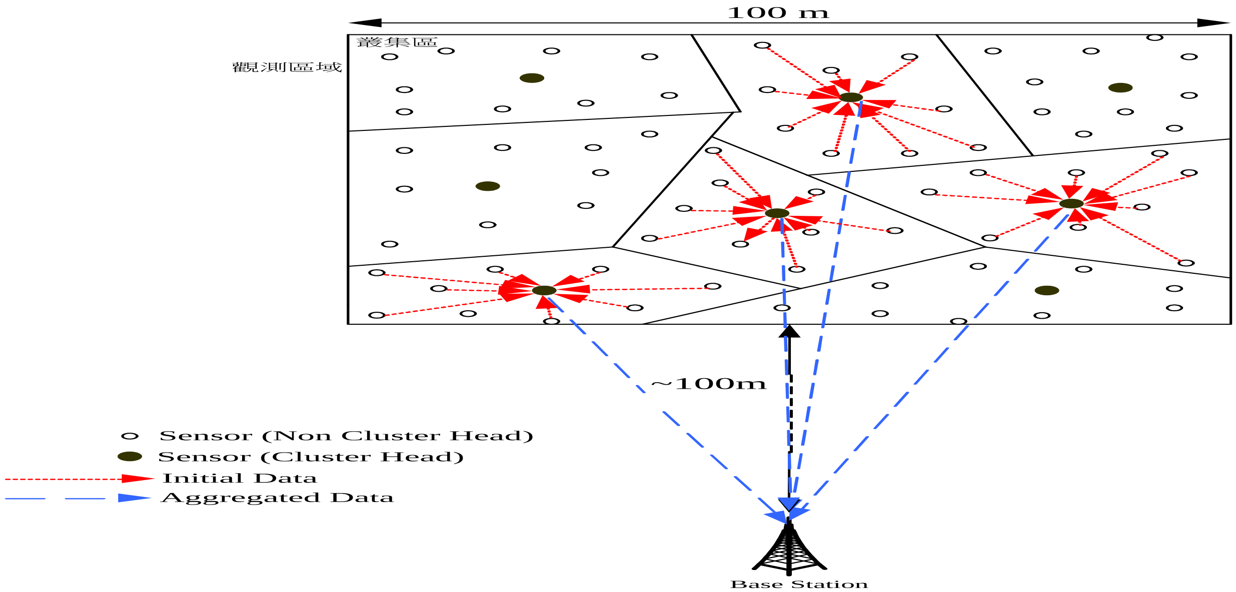


Fig. 2. Architecture of Wireless Sensor Network.

Actually combining sensors, radios, and CPU's into an effective wireless sensor network requires a detailed understanding of the both capabilities and limitations of each of the underlying hardware components, as well as a detailed understanding of modern networking technologies and distributed systems theory. Each individual node must be designed to provide the set of primitives necessary to synthesize the interconnected web that will emerge as they are deployed, while meeting strict requirements of size, cost and power consumption. A core challenge is to map the overall system requirements down to individual device capabilities, requirements and actions. To make the wireless sensor network vision a reality, architecture must be developed that synthesizes the envisioned applications out of the underlying hardware capabilities. To develop this system architecture we work from the high level application requirements down through the low-level hardware requirements. In this process we first attempt to understand the set of target applications. To limit the number of applications that we must consider, we focus on a set of application classes that we believe are representative of a large fraction of the potential usage scenarios. We use this set of application classes to explore the system-level requirements that are placed on the overall architecture. From these system-level requirements we can then drill down into the individual node-level requirements. Additionally, we must provide a detailed background into the capabilities of modern hardware. After we present the raw hardware capabilities, we present a basic wireless sensor node.

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 *ECH init* and *ESN init* 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 *A*2. 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 λCH and λSN, respectively, with $\lambda CH < \lambda SN$. The radio ranges used by CH and SN transmission is denoted by *rCH* and *rSN*, 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 multihop routing. Due to limited energy, a packet is sent hop by hop without using acknowledgment or retransmission [2].



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* [25] when performing packet routing to disrupt the operation of the network. Environment conditions which could cause a node to fail with a certain probability include hardware failure (q), and transmission failure due to noise and interference (e). Moreover, the hostility to the HWSN is characterized by a per-node capture rate of λc which can be determined based on historical data and knowledge about the target application environment.
These probabilities are assumed to be constant and known at deployment time.

IV. Mathematical Model

We develop a mathematical model to estimate the MTTF of a HWSN using multipath data forwarding for answering queries issued by a mobile user roaming in the HWSN area. The basic idea of our MTTF formulation is to we 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. As the system dynamically evolved, the amount of energy spent per query also varies dynamically.

A. Network Dynamic:

Initially at deployment time all nodes (CHs or SNs) are good nodes. 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.

B. Query Success Probability:

We will use the notation *SNj* to refer to *SN j* and *CHj* to refer to *CHj*. There are three ways by which data forwarding from *CHj* to *CHk* could fail: (a) transmission speed violation; (b) sensor/channel failures; and (c) *CHj* is compromised. The first source of failure, transmission speed violation, accounts for query deadline violation.

V. Analysis

Our example HWSN consists of 3000 SN nodes and 100 CH nodes, deployed in a square area of *A*2 (200*m* × 200*m*). Nodes are distributed in the area following a Poisson process with density *λSN* = 30 nodes/(20 × 20 *m*2) and *λCH* = 1 node/(20×20 *m*2) at deployment time. The radio ranges *rSN* and *rCH* are dynamically adjusted between 5m to 25m and 25m to 120m respectively to maintain network connectivity. The initial energy levels of SN and CH nodes are *ESN* 0 = 0.8 Joules and *ECH* 0 = 10 Joules so that thThe correctness of our protocol design is evidenced by the effect of *Tcomp*, *m*, and *TIDS* on optimal (*mp*,*ms*). show MTTF vs. (*mp*,*ms*) under low and high attack rates, respectively. First of all, in both graphs, we observe the existence of an optimal (*mp*,*ms*) value under which MTTF is maximized. Secondly, there exists an optimal *m* value (the number of voters) to maximize MTTF. In Fig. 10, *m* = 7 yields a higher MTTF value than *m* = 3 because in this scenario the attack rate is relatively high (one in four days), so a higher number of voters is needed to cope with and detect bad nodes more effectively, to result in a higher query success rate and thus a higher MTTF.ey exhaust energy at about the same time.

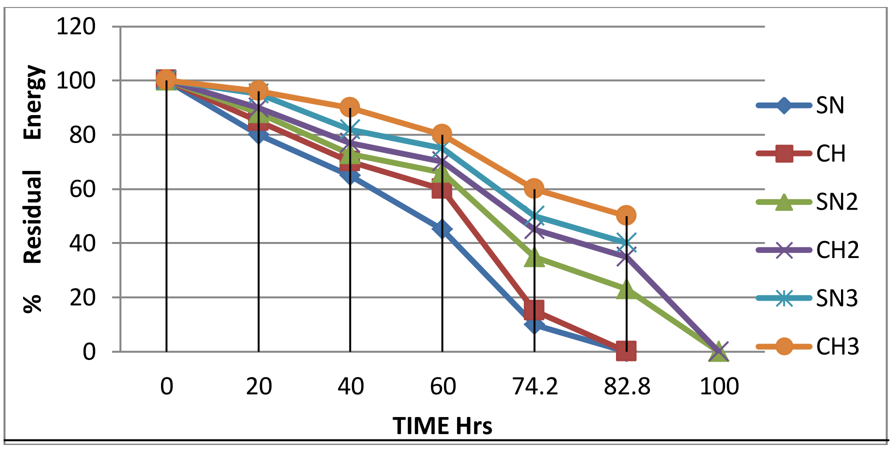


Fig :Effect of (*mp*,*ms*) on energy of CHs and SNs.

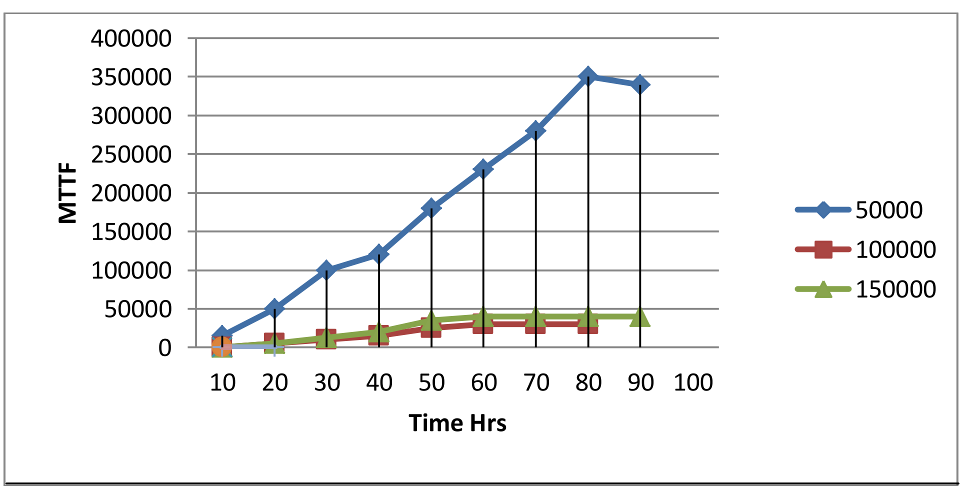


Fig:Effect of (*mp*,*ms*) on MTTF.

VI. Conclusion And Future Work

The goal is to satisfy the application QoS requirements to continuous life time of sensor system. And to improve mathematical model for lifetime sensor systems by using two function system parameter such as source and path redundancy levels. The basic idea behind this is to reuse available system information which variety layer stack. Adaptive network management with three countermeasures for coping with selective captures aiming to create holes near the base station in a wireless sensor network to block data delivery. Our countermeasures are effective against selective capture.Radio adjustment, the best redundancy level for multipath routing, the best number of voters, and the best intrusion invocation interval used for intrusion detection to maximize the system lifetime. Our future work, we plan to explore more extensive diverse 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. To strengthen intrusion detection through "weighted voting" leveraging knowledge of trust/reputation of neighbor nodes, And to tackle the "what paths to use" problem in multipath routing decision making for intrusion tolerance in WSNs. we plan to explore trust-based admission control [38]–[40] to optimize application performance.

REFERENCES

[1]Hamid Al-Hamadi and Ing-Ray Chen (2013) „Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks‟ Vol 10.

[2] 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

[3] 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, 2011.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] S. T. Cheng, C. M. Chen, and I. R. Chen, "Performance evaluation of an admission control algorithm: dynamic threshold with negotiation," *Performance Evaluation*, vol. 52, no. 1, pp. 1–13, 2003.

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

[10] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "Anapplication-specific protocol architecture for wireless microsensor *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–6702002.

[11] I. R. Chen and T. H. Hsi, "Performance analysis of admission controlalgorithms based on reward optimization for real-time multimedia

servers," *Performance Evaluation*, vol. 33, no. 2, pp. 89–112, 1998.

[12] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans. MobileComput.*, vol. 3, no. 4, pp. 366–379, 2004.

BIOGRAPHY

Shaik Tanveer sultana is a student in Master of Technology in the Department of Computer Science and Engineering, Bharath College of engineering and technology for women, kadapa, Andhra Pradesh, India.

S.Rajiya Sulthana is an Assistant Professor in the Department of Computer Science and Engineering, Bharath College of engineering and technology for women, kadapa, Andhra Pradesh, India.