Multipath secure routing for intrusion tolerance in heterogeneous wireless sensor networks

S.D.Sujitha Rajakumari[1], T.Kadhambari[2], J.Dolly Irene[3]

[1] **M.E.Communication System, Prathyusha Institute of Technology and Management,**
Chennai, Tamil Nadu, India

[2,3]**Assistant Professor, E.C.E Department, Prathyusha Institute of Technology and Management,**
Chennai, Tamil Nadu, India

Abstract

To propose redundancy management of heterogeneous wireless sensor networks (HWSNs), utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of our redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. Furthermore, we consider this 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. To analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voters and the intrusion invocation interval under which the lifetime of a HWSN is maximized.

Key words: Heterogeneous wireless sensor networks, multipath routing, intrusion detection, reliability, security, energy conservation.

1.Introduction

Wireless sensor networks are deployed in an unattended environment in which energy replenishment is difficult if not impossible. Due to limited resources, a WSN must not only satisfy the application specific QoS requirements such as reliability, timeliness and security, but also minimize energy consumption to prolong the system useful lifetime. The tradeoff between energy consumption vs reliability gain with the goal to maximize the WSN system lifetime has been well explored in the literature. However, no prior work exists to consider the tradeoff in the presence of malicious attackers.

Using homogeneous nodes which rotate among themselves (CHs) and sensor nodes (SNs) leveraging CH election protocols such as HEED [1] for lifetime maximization has been considered [2]. Using heterogeneous nodes can further 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. The tradeoff issue between energy consumption vs. QoS gain becomes much more complicated when inside attackers are present as a path may be broken when a malicious node is on the path. This is especially the case in heterogeneous WSN (HWSN) environments in which CH nodes may take a more critical role in gathering and routing sensing data. Thus, very likely the system would employ an intrusion detection system (IDS) with the goal to detect and remove malicious node .Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. It satisfies the energy consumption through turn off the sensor nodes for period of time to save energy. The basic idea is that the probability of at least one path reaching the sink node or base station increases as we have more paths doing data delivery. While most prior research focused on using multipath routing to improve reliability [3], some attention has been paid to using multipath routing to tolerate insider attacks. These studies, however, largely ignored the tradeoff between QoS gain vs. energy consumption which can adversely shorten the system lifetime. The research problem we are addressing in this paper is effective redundancy management of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes.

2. System model

In Cluster-based WSN Architecture , the deployment typically through air-drop SNs are homogeneous with same initial energy level E_0.Assume deployment area is A^2.SNs are distributed with a homogeneous spatial Poisson process with intensity λ .Domain is free of obstacles but SNs have constant hardware and software Failure probabilities (each between 0 and 1)[4].SNs form Clusters and each cluster has a CH. The role of CH to manage the network within the cluster to gather sensor data from SNs . An aggregation of readings, relay data to the PC sometimes duplicate packets arrive and single packet forwarded .Users issue queries through any CH.CH that receives the query is called the Processing Center (PC).Queries assumed to be issued on the move, hence tight timeliness requirements. Queries arrive in accordance with a Poisson process with rate, May involve multiple clusters (termed source clusters).Transmission power reduced to minimum level (enough for one-hop radio range, *r*) . Can increase with time dynamically when network becomes less dense. Routing is based on Geographic routing. No path information maintained by individual SNs. Location of neighboring node known to a sending node. All nodes receive and maintain location of CH (through voting process) .

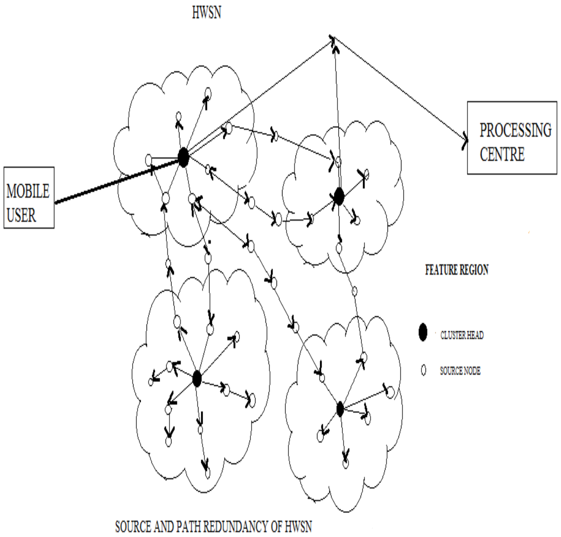

fig.1

3. Probability Model

The 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. To find best redundancy level (m_s, m_p) that maximizes MTTF, while satisfying query reliability (R_{req}) and timeliness (T_{req}) , requirements .

$$R_q > R_{req}$$

Implicitly satisfies timeliness (T_{req}) requirement. Maximum number of queries that can be answered before queries. The probability that the first i queries are successful but the (i+1)the query failure is taken as

$$R_q^i \ * (1- R_q)$$

.The expected number of queries that the system can answer without experiencing the failure with the upper bound of $N_{q\ldots\text{Each}}$ query .has a reliability of R_q.Finally MTTF as the probability weighted average of the number of queries can handle without experiencing a without experiencing any deadline, transmission, or security failure

$$\text{MTTF}= \sum_{i-1}^{N_q-1} iR_q^i\left(1-R_q\right)+ N_qR_q^{N_q}$$

MTTF formulation is that to deduce the maximum number of queries,N_q are processed successfully without any failure for which the system will have the longest lifetime span. Energy consumption is to estimate through amount of energy consumed by transmission and reception over wireless link.

$$E_q = \sum_{k=1}^{np} E_q\,(k)P_q(k)$$

$P_q(k)$ is probability that a query requires k source clusters to respond, $E_{q(k)}$ is energy consumption of the system to answer a query that requires k source clusters. SNs operate in power saving mode to save energy in Active mode or Sleep mode Energy to transmit a data packet of length $n_b$bits a distance *r(m)*

$$E_T = n_b(E_{elec} + E_{amp}r^2)$$

Where , $E_{elec}$is Energy to run the transmitter and receiver circuitry (J/bit). E_{amp} is Energy used by the transmit amplifier to achieve an acceptable signal to noise ratio (J/bit/m2). r^2 is energy loss due to channel transmission, Energy to receive a message ,

$$E_R = n_b E_{elec}$$

For transmission and reception energy consumption of sensors, adopt energy model in CH and SN. Lastly, for intrusion detection every node is evaluated by an *m* voters and the knowledge of $N_q$to calculate the system MTTF given by equation.

Performance Evaluation

HWSN consists of 3000 SN nodes and 100 CH nodes, deployed in a square area of $A_2(200m \times 200m)$. Nodes are distributed in the area following a Poisson process with density SN = 30 nodes/(20 × 20 m_2) and CH = 1node/(20×20 m_2) at deployment time. The radio ranges r_{CH} and r_{SH} 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 E_{SN0}= 0.8 Joules and E_{CH0}= 10 Joules so that they exhaust energy at about the same time. The energy dissipation to run the transmitter and receiver circuitry is 50 nJ/bits.The energy used by the transmit amplifier to achieve and acceptable signal to noise ratio.Fig.2&3 shows an optimal combination (m_p, m_s)under low and high capture rate for lifetime maximization.

5. Existing system

In exiting system, the optimum communication range and communication mode were derived to maximize the network lifetime. A voting based distributed intrusion detection is applied to remove malicious nodes from the HWSN .In some clustering algorithm, unsatisfactory cluster formations, which may cause the network to suffer from load imbalance or extra energy consumption.

Voting-based Clustering Algorithm (VCA) for energy-efficient data dissemination in wireless sensor networks. This new approach lets sensors vote for their neighbors to elect suitable cluster heads. VCA is completely distributed, location unaware and independent of network size and topology. It combines load balancing, energy and topology information together by using very simple voting mechanisms. Simulation results show that VCA can reduce the number of clusters by 5-25% and prolong the lifetime of a sensor network by 10-30% over that of existing energy-efficient clustering protocols.

6.Proposed system

To explore more extensive malicious attacks in addition to packet dropping and bad mouthing attacks and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks The Effects of T_{IDS} on MTTF under low capture rate and high capture rate is shown in Fig (2) & Fig(3)

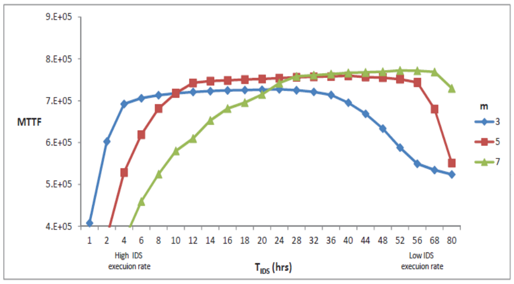

Fig.2 Effect of T_{IDS} on MTTF under low capture rate

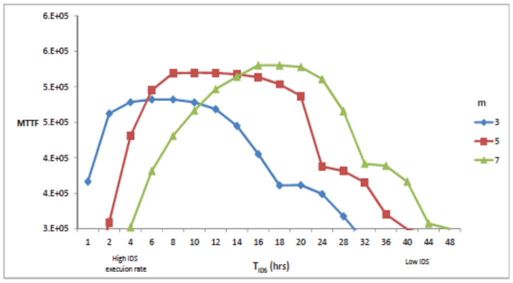

Fig.3 Effect of T_{IDS} on MTTF under low capture rate

Another direction is to consider targeted attacks, capture certain strategic nodes with higher probability and malicious behavior and collude with other attackers to avoid intrusion detection.

Reference

[1] 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 Manag.*,vol. 9, no. 2, pp. 161–183, 2012.

[2] E. Stavrou and A. Pitsillides, “A survey on secure multipath routing protocols in WSNs,” *Comput. Netw.*, vol. 54, no. 13, pp. 2215–2238, 2010.

[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] 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.

[5] 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. Reliab.*, vol. 59, no. 1, pp. 231–241, 2010