International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 22-28
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

REDUNDANCY MANAGEMENT OF MULTIPATH ROUTING FOR INTRUSION TOLERANCE IN HETEROGENEOUS WIRELESS SENSOR NETWORKS

Mrs.A.Sangeetha M.E.[+]., Ms.P.Praveena M.E(CSE) *
*- *Department of Computer Science and Engineering, PGPCET, Namakkal.*
+- *Assistant Professor, Department of Computer Science and Engineering, PGP College of Engineering and Technology, Namakkal*

ABSTRACT

In this paper we propose redundancy management of heterogeneous wireless sensor networks (HWSNs), utilizing multipath routing to answer user queries in the presence ofunreliable 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. We develop a novel probability model 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. We then apply 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

1. INTRODUCTION

Many wireless sensor networks (WSNs) 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.

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 nodes. While the literature is abundant in intrusion detection techniques for WSNs [7-11], the issue of how often intrusion detection should be invoked for energy reasons in order to remove potentially malicious nodes so that the system lifetime is maximized (say to prevent a Byzantine failure [12]) is largely unexplored. The issue is especially critical for energy constrained WSNs designed to stay alive for a long mission time.

Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is that the probability of at least one pathreaching 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 [2, 3, 13], some attention has been paid to

International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 22-28
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

using multipath routing to tolerate insider attacks [14-16].

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. We address the tradeoff between energy consumption vs. QoS gain in reliability, timeliness and securitywith the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. More specifically, we analyze the optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime. 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-basedanalysis 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. 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. To the best of our knowledge, we are the first to address the "how many paths to use" problem. For the "what paths to use" problem, our approach is distinct from existing work in that we do not consider specific routing protocols (e.g., MDMP for WSNS [17] or AODV for MANETs [18]), nor the use of feedback information to solve the problem. Rather, for energy conservation, we employ a distributed light-weight IDS by which intrusion detection is performed only locally. Nodes that are identified compromised are removed from the HWSN. Only compromised nodes that survive detection have the chance to disturb routing. One main contribution of our paper is that we decide "how many paths to use" in order to tolerate residual compromised nodes that survive our IDS, so as to maximize the HWSN lifetime.

2. RELATED WORK

Over the past few years, many protocols exploring the tradeoff between energy consumption and QoS gain particularly in reliability in HWSNs have been proposed. In [19], the optimal communication range and communicationmode were derived to maximize the HWSN lifetime. In [20],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 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. In [21], 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 to [21] our work also considers heterogeneous nodes with different densities and capabilities. However, 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.

In the context of secure multipath routing for intrusion tolerance, [22] provides an 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. In [14] the authors considered a disjoint multipath routing protocol to tolerate intrusion using multiple disjoint paths in WSNs. Our work also uses multipath routing to tolerate intrusion. However, we specifically consider energy being consumed for intrusion detection, and both CHs and SNscan be compromised for lifetime maximization. In [23] a randomized dispersive multipath routing protocol is proposed to avoid black holes.

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 raisealarms if the number of failures exceeds a threshold value, so if a monitor node is malicious, it can quickly infect others. In [8], a collaborative approach is proposed forintrusion detection where the decision
is based on a majority voting of monitoring nodes.

In general there are two approaches by which energyefficient 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 neighbour

International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 22-28
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

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 monitoringneighbor SNs and CHs monitoringneighbor 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. 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.

3. 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. Anycommunication 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 the 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 *packetdropping 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 pernodecapture rate of λ_c 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.

Redundancy management:

Redundancy management of multipath routing for intrusiontolerance is achieved through two forms of redundancy: (a) source redundancy by which m_sSNs sensing a physicalphenomenon in the same feature zone are used to forwardsensing data to their CH (referred to as the source CH); (b) pathredundancy by which m_p paths are used to relay packets from the source CH to the PC through intermediate CHs.

Fig. 1shows a scenario with a source redundancy of 3 (m_s= 3) and a path redundancy of 2 (m_p= 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 $m_p$and m_s, we can effectively result in $m_p$redundant paths for path redundancy and $m_s$distinct paths from $m_s$sensors for source redundancy. Cluster head Sensor node

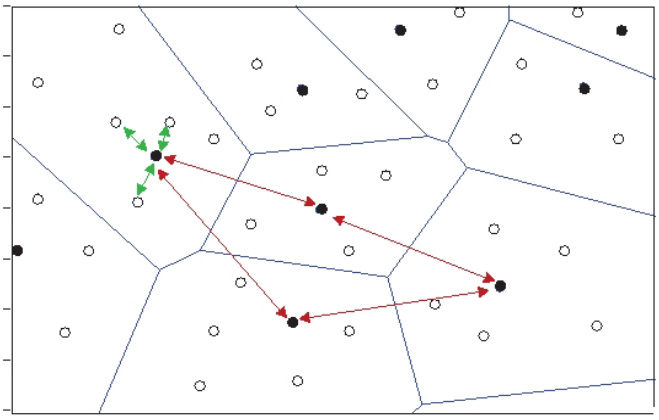

Figure. 1: Source and Path redundancy for a Heterogeneous WSN.

We assume that geographic routing [18], a well-known routing protocol for WSNs, is used to route the information between nodes; thus, no path information is maintained. The location of the destination node needs to be known to correctly forward a packet. As part of clustering, a CH knows the locations of SNs within its cluster, and vice versa. A CH also knows the location of neighbor CHs along the direction towards the processing center. We

International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 22-28
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

assume that sensors operate in power saving mode. Thus, a sensor is either active (transmitting or receiving) or in sleep mode. For the transmission and reception energy consumption of sensors, we adopt the energy model in [1] for both CHs and SNs.

Multipath routing

Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. 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.Multi-path routing protocols establish multiple disjoint paths from asource to a destination and are thereby improving resilience to network failures.to ensure that a data packet correctly send to the destination, it used of an improved hybrid method based on multipath data sending.

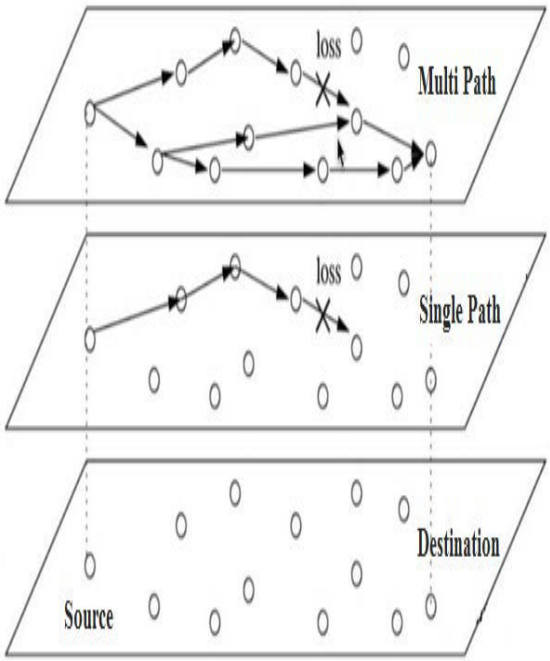

Figure:2 Multi Path Sending

The routing decisions in this method are by considering the remaining energy of nodes that are in neighbors of sender nodes. Simulation results shows that release rate of data packets in this method is reduced and reliability in data sending to destination is increased. Also, the energy efficiency of sensor nodes effectively improved and thus increase the overall lifetime of wireless sensor networks. In multi path sending methods for access to required reliability, the same copies of a packet send through multiple routes. if the numbers of needed neighbours were not enough, other copy of the packet sent through repetitive paths. So that, more copies of packets are sent via the same route.

Intrusion detection:

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. 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 votingbased distributed IDS is applied periodically in every 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 pairwise keys. When the majority of voters come to the conclusion that a target node is bad, then the target node is evicted.For both CHs and SNs, there is a system-level false positive probability that the voters can incorrectly identify a good node as a bad node. There is also a system-level false negative probability that the voters can incorrectly misidentify a bad node as a good node. These two system-level IDS probabilities will be derived based on the *bad-mouthing* attack model in the paper.

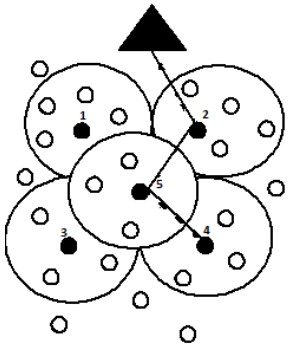

Figure:3 Routing path establishment

International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 22-28
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

In our malicious node detection technique we use a monitoring mechanism. In this mechanism when a node *A* sends message to node *B*, it converts itself to a monitoring mode we refer here as A_m. Due to the broadcast nature of wireless sensor networks A_m monitors the behavior of node *B* after sending the message. When node B transmits the message to the next node, A_m hears that and compares with the message it has sent to node *B*, hence establishing *original* and *actual* message. If the message transmitted by node *B* is *original* then node A_m ignores it and continues with its own tasks but if there is a difference between *original* and *actual* messages greater than a threshold, the message is considered as suspicious and node *B* is now considered as a suspicious node B_s.

Each node builds a *node suspicious* table containing the reputation of nodes in the cluster. Entries in this table contain the node ID, and the number of suspicious and unsuspicious entries. Nodes update this table every time it identifies a suspicious activity by increasing suspicious count by one for that particular node. In Table II below ID is the unique ID of sensor node; *NS* denote node suspicious and *NU* node unsuspicious entries.

Table :1 Node Suspicious Table

Node ID	Suspicious entries	Unsuspicious entries
ID	NS>1	NU>1

Here we note that increasing source or path redundancyenhances reliability and security. However, it also increases theenergy consumption, thus contributing to the decrease of the system lifetime. Thus, there is a trade-off between reliability/security gains vs. energy consumption. The distributed IDS design attempts to detect and evict compromised nodes from the network without unnecessarily wasting energy so as to maximize the query success probabilityand the system lifetime.

To provide a unifying metric that considers the above two design tradeoffs, we define the total number of queries the system can answer correctly until it fails as the *lifetime* or the *mean time to failure* (MTTF) of the system, which can be translated into the actual system lifetime span given the query arrival rate. A failure occurs when no response is received before the query deadline. The cause could be due to energy exhaustion, packet dropping by malicious nodes, channel/node failure, or insufficient transmission speed to meet the timeliness requirement. Our aim is to find both the optimal redundancy levels and IDS settings under which the MTTF is maximized, when given a set of parameters characterizing the operational and environment conditions.

4. 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 sensor networks utilizing multipath routing to answer user queries. We developed a novel probability model to analyze the best redundancy level in terms of 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 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 ofunreliable wireless communication and malicious nodes. Finally, we applied our analysis results 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 prolong the system lifetime.

REFERENCES

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

[2] E. Felemban, L. Chang-Gun, and E. Ekici, "MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness inwireless 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-TolerantQoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks," *IEEE Trans. on Dependable andSecure Computing*, vol. 8, no. 2, pp. 161-176, 2011.

[4] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S.Singh, "Exploiting heterogeneity in sensor networks," *24th Annu. Joint*

International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 22-28
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

*Conf. of the IEEE Computer and Communications Societies (INFOCOM),*2005, pp. 878-890 vol. 2.

[5] H. M. Ammari and S. K. Das, "Promoting Heterogeneity, Mobility, andEnergy-Aware Voronoi Diagram in Wireless Sensor Networks," *IEEETrans. Parallel Distrib. Syst.*, vol. 19, no. 7, pp. 995-1008, 2008.

[6] X. Du and F. Lin, "Improving routing in sensor networks withheterogeneous sensor nodes," *IEEE 61st Vehicular TechnologyConference*, 2005, pp. 2528-2532.

[7] S. Bo, L. Osborne, X. Yang, and S. Guizani, "Intrusion detectiontechniques in mobile ad hoc and wireless sensor networks," *IEEEWireless Commun.*, vol. 14, no. 5, pp. 56-63, 2007.

[8] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detectionin wireless sensor networks," *13th European Wireless Conference*, Paris,France, 2007.

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

[10] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L.B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wirelesssensor networks," *1st ACM Workshop on Quality of Service & Securityin Wireless and Mobile Networks*, Montreal, Quebec, Canada, 2005.

[11] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: asurvey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6-28, 2008.

[12] L. Lamport, R. Shostak, and M. Pease, "The Byzantine GeneralsProblem," *ACM Trans. Programming Languages and Systems*, vol. 4, no.3, pp. 382-401, 1982.

[13] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliabledisjoint and braided multipath routing for sensor networks," *J. NetwComput. Appl.*, vol. 33, no. 4, pp. 422-432, 2010.

[14] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing forwireless sensor networks," *Computer Communications*, vol. 29, no. 2, pp.216-230, 2006.

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

[16] W. Lou and Y. Kwon, "H-SPREAD: a hybrid multipath scheme forsecure and reliable data collection in wireless sensor networks," *IEEETrans. Veh. Technol.*, vol. 55, no. 4, pp. 1320-1330, 2006.

[17] Y. Lan, L. Lei, and G. Fuxiang, "A multipath secure routing protocolbased on malicious node detection," *Chinese Control and DecisionConference*, 2009, pp. 4323-4328.

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

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

[20] I. Slama, B. Jouaber, and D. Zeghlache, "Optimal Power managementscheme for Heterogeneous Wireless Sensor Networks: LifetimeMaximization under QoS and Energy Constraints," *Third InternationalConference on Networking and Services (ICNS)* 2007, pp. 69-69.

[21] R. Machado, N. Ansari, G. Wang, and S. Tekinay, "Adaptive densitycontrol in heterogeneous wireless sensor networks with and withoutpower management," *IET Communications*, vol. 4, no. 7, pp. 758-767,2010.

[22] E. Stavrou and A. Pitsillides, "A survey on secure multipath routingprotocols in WSNs," *Comput. Netw.*, vol. 54, no. 13, pp. 2215-2238,2010.

[23] T. Shu, M. Krunz, and S. Liu, "Secure Data Collection in Wireless SensorNetworks Using Randomized Dispersive Routes," *IEEE Trans. Mobile Comput.*, vol. 9, no. 7, pp. 941-954, 2010.

[24] Y. X. Jiang and B. H. Zhao, "A Secure Routing Protocol with MaliciousNodes Detecting and Diagnosing Mechanism for Wireless

International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 22-28
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

SensorNetworks," *Asia-Pacific Service Computing Conference, The 2nd IEEE,*2007, pp. 49-55.

[25] 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.

[26] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: reliable informationforwarding using multiple paths in sensor networks," *28th IEEE LocalComputer Networks*, Bonn, Germany, 2003, pp. 406-415.

[27] G. Bravos and A. G. Kanatas, "Energy consumption and trade-offs onwireless sensor networks," *16th IEEE Int. Symp. on Personal, Indoor andMobile Radio Communications* 2005, pp. 1279-1283.

[28] S. Qun, "Power Management in Networked Sensor Radios A NetworkEnergy Mode *IEEE Sensors Applications Symp.*, 2007, pp. 1-5.

[29] C. Haowen and A. Perrig, "PIKE: peer intermediaries for keyestablishment in sensor networks," *24th Annu. Joint Conf. of the IEEEComputer and Communications Societies.*, 2005, pp. 524-535.

[30] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms forlarge-scale distributed sensor networks," *10th ACM conference onComputer and Communications Security*, Washington D.C., USA, 2003.

[31] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensornetworks," *J. High Speed Netw.*, vol. 15, no. 1, pp. 33-51, 2006.

[32] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly detection inwireless sensor networks," *IEEE Wireless Communications*, vol. 15, no.4, pp. 34-40, 2008.

[33] F. Bao, I. R. Chen, M. Chang, and J. Cho, "Hierarchical TrustManagement 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.

[34] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchicalclustering algorithm for wireless sensor networks " *22nd Conf. of IEEEComputer and Communications*, 2003, pp. 1713-1723.

[35] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "Anapplication-specific protocol architecture for wireless microsensornetworks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660-670,
2002.

[36] C. J. Fung, Z. Jie, I. Aib, and R. Boutaba, "Dirichlet-Based TrustManagement for Effective Collaborative Intrusion Detection Networks,"*IEEE Trans. Netw. Service Manag.*, vol. 8, no. 2, pp. 79-91, 2011.

[37] S. Ozdemir, "Secure and reliable data aggregation for wireless sensornetworks," *Proceedings of the 4th international conference on Ubiquitous computing systems*, Tokyo, Japan, 2007.

[38] I. R. Chen and T. H. Hsi, "Performance analysis of admission controlalgorithms based on reward optimization for real-time multimediaservers," *Performance Evaluation*, vol. 33, no. 2, pp. 89-112, 1998.

[39] S. T. Cheng, C. M. Chen, and I. R. Chen, "Dynamic quota-basedadmission control with sub-rating in multimedia servers," *Multimediasystems*, vol. 8, no. 2, pp. 83-91, 2000.

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