Intrusion Detection & Fault Tolerance in Heterogeneous Wireless Sensor Network: A Survey

Sneha Dhage*, Purnima Soni**

* Computer Science & Engineering, G.H. Raisoni Institute of Engineering and Technology for Women, Nagpur.

** Computer Science & Engineering, G.H. Raisoni Institute of Engineering and Technology for Women, Nagpur.

Abstract- Research problems are to enhance an Intrusion Detection System (IDS) of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes. Also, to address the energy consumption and QoS gain in reliability, delay and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. The proposed research is a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes. The proposed work consider multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node. System describes a heterogeneous WSN comprising a large number of sensor nodes with vastly different social and quality of service (QoS) behaviors with the objective to yield "ground truth" node status through "weighted voting" leveraging knowledge of trust/reputation of neighbor nodes. To demonstrate the utility of the hierarchical trust management protocol, it can be apply to trust-based intrusion detection and trust-based geographic routing. For trust-based intrusion detection, there exists an optimal trust threshold for minimizing false positives and false negatives probability. Furthermore, trust-based intrusion detection outperforms traditional anomaly-based intrusion detection approaches in both the detection probability and the false positive probability. The proposed research also present a new multipath routing protocol which provides strong fault tolerance by increasing the number of constructed paths up to four times, as well as tackle the "what paths to use" problem in multipath routing decision making for intrusion tolerance in WSNs. The protocol relies on a new multipath constructions paradigm that is defined specifically for heterogeneous WSN. The approach leverages a reasonable increase in the network lifetime and a higher resilience and fault tolerance.

Index Terms- Intrusion detection system (IDS), multipath routing, fault tolerance, trust management, heterogeneous WSN (HWSN)

I. INTRODUCTION

Advances in wireless communication and miniature electronics have enabled the development of small, low-cost, low-power sensor nodes (SNs) with sensing and communication capabilities. Therefore, the issues of Wireless Sensor Networks (WSNs) have become popular research subjects. WSN is infrastructure based network, and through the mass deployment of SNs, a WSN is formed. The major function of WSN is to collect and monitor the related information which about the specific environment. The SNs detect the surrounding environment or the given target and deliver the data to the sink using wireless communication. The data is then analyzed to find out the state of the target. However, due to the design of their hardware, WSNs suffer from many resource constraints, such as low computation capability, limited memory and limited energy. Because WSNs are composed by numerous low-cost and small devices which are usually deploy to an open and unprotected area, they are vulnerable to various types of attacks. A prevention mechanism is used to counteract well-known attacks. However, prevention mechanisms cannot resist overall attacks. Therefore, the attacks are required to be detected. An Intrusion Detection System (IDS) is used frequently to detect the packets in a network, and determine whether they are attackers. Additionally, IDS can help to develop the prevention system through acquired natures of attack. Many wireless sensor networks (WSNs) are deployed in an unattended environment in which energy replenishment is difficult. Due to limited resources, a WSN must not only satisfy the application specific QoS requirements such as reliability, minimum delay and security, but also minimize energy consumption to prolong the system useful lifetime.

Recently, prior research efforts have been made to develop network architectures and sensor hardware in order to effectively deploy WSNs for a variety of applications. However, Due to a wide diversity of WSN application requirements, a general-purpose WSN design cannot fulfill the needs of all applications. Network parameters such as sensing range, node density and transmission range have to be carefully considered according to specific applications, at the network design stage. In order to achieve this, it is essential to capture the impacts of network parameters on network performance with respect to

application specifications. Intrusion detection (i.e., object tracking) in a WSN can be regarded as a monitoring system for detecting the intruder that is invading the network domain. Thus, it is necessary to develop the intrusion detection system (IDS) which is capable of handling more extensive malicious attacks with energy conservation mechanism to increase system lifetime.

In a WSN, there are two ways for the detection of an intruder: single-sensing detection and multiple-sensing detection. The intruder can be successfully detected by only a single sensor, in the single-sensing detection. On the other hand, in the multiple-sensing detection the intruder can only be detected by multiple sensors. In some applications; the sensed information provided by a single sensor might not be adequate for recognizing the intruder, because single sensors can only sense a portion of the intruder. 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. Cluster-based Wireless Sensor Network (CWSN) is shown in Figure 1.

Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data communication and data delivery in WSNs. Most prior research focused on using multipath routing to improve reliability [5], [6], and to tolerate insider attacks [7].However, these studies largely ignored energy consumption which can adversely shorten the system lifetime. The research problems are to enhance an Intrusion Detection System (IDS) of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes. Also, to address the energy consumption and QoS gain in reliability, minimum delay and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS 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 data delivery success probability is maximized while maximizing the HWSN lifetime.

II. RESEARCH ELABORATIONS

Over the past few years, many protocols exploring the energy consumption and QoS gain particularly in reliability in HWSNs have been proposed. In [8], the optimal communication range and communication mode were derived to maximize the HWSN lifetime. In [9], the authors devised intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a HWSN with CH nodes having larger energy and processing capabilities than normal 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 [8], [9], no consideration was taken in to the account about the existence of malicious nodes in the network. Relative to [9] the proposed work considers heterogeneous nodes with different densities and capabilities. However, the work also 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.

Compared with existing works cited above, 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 90% - 95% accuracy and 90% - 94% 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.

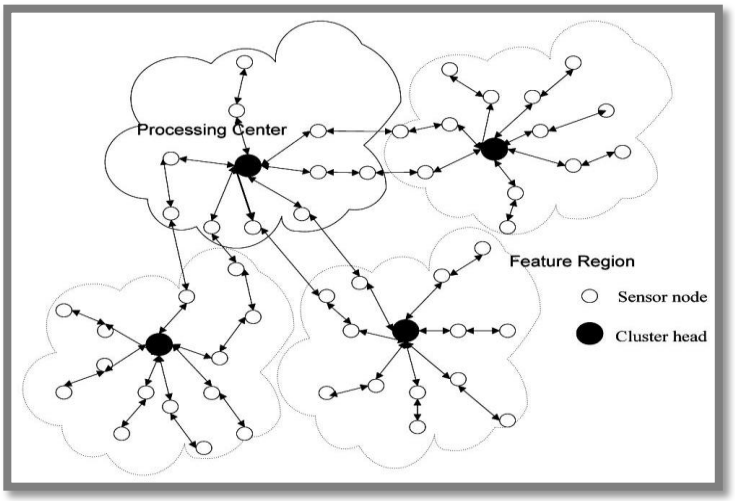

Figure 1 : Cluster-based WSN Architecture.

III. CONCLUSION

The proposed hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two aspects of trustworthiness, namely, social trust and QoS trust. The research work will include the development of a probability model utilizing various techniques to analyze the protocol performance, and validated subjective trust against objective trust obtained based on ground truth node status. Based on the protocol the algorithm for trust-based intrusion detection will be developing

using weighted voting. The algorithm will identify the best way to form trust out of social and QoS trust properties (i.e., identifying weights to assign to individual trust properties) and to assign the minimum trust threshold, so that the performance of trust-based intrusion detection is maximized, i.e., both false positives and false negatives are minimized.

Also, the research will deal with the challenging issue of providing fault tolerance in wireless sensor networks. Firstly a new multipath paradigm for heterogeneous wireless sensor networks will be define and analyzes upon various parameters. Then, propose a new fault tolerant multipath routing protocol which discovers an important number of energy node disjoint paths with the slightest overhead of one message per node. Intensive simulations will be conducted to evaluate our protocol with different scenarios, sensor nodes densities and deployment strategies.

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, 2011.

[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 (ISCIT), pp. 4673-1157.

AUTHORS

First Author Sneha Dhage has received her B.E. degree in Computer Technology from K.D.K. College of Engineering, RTMNU University in 2010. She is pursuing M.E. in Wireless Communication and Computing from G.H.Raisoni Institute of Engineering and Technology for Women Nagpur.
E-mail: snehadhage2009@gmail.com

Second Author Purnima Soni, Assistant Professor in Department of Computer Science and Engineering @ G.H. Raisoni Institute of Engineering and Technology for Women Nagpur. She has pursued her M.E in Wireless Communication & Computing from G.H. Raisoni College of Engineering Nagpur.
E-mail: Purnima_456@yahoo.com