IPHV7I20018X

International Journal Of Advanced Research and Innovation -Vol.7, Issue .II

ISSN Online: 2319 – 9253

Print: 2319 – 9245

ROBUST MODULE TO MANAGE EXCESS STUFF ON MULTI PATH ROUTING FOR PROVIDING INCURSION STRENGTH IN WSN'S.

#1R.LOHITHA-M.Tech Student,
#2 B.Mahesh- Asst.Professor,

Department of Computer Science and Engineering,

Dr.K.V.Subba Reddy College Of Engineering For Women , Kurnool,A.P

Abstract- Research problems are to enhance an Intrusion Detection System (IDS) of a clustered HWSN to prolong its lifetime operation and performance of the system in the presence of and malicious nodes. Also, to address the energy consumption, gain in reliability, delay and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements. The proposed research is a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with unreliable or malicious nodes. The proposed work considers 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 system. 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 makes use of AOMDV routing protocol which provides strong fault 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- Fault tolerance, Heterogeneous WSN (HWSN), Intrusion detection system(IDS), Multipath Routing, Trust Management.

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. Thus, the issues of Wireless Sensor Networks (WSNs) have become popular research subjects. WSN is infrastructure based Network, the mass deployment of SNs is done in WSN and network 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 structure of WSN and 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,remote 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 malicious packet or 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 is requires to satisfy the application specific QoS requirements such as reliability, minimum delay and security, and 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 very essential to capture the impacts of various 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 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.

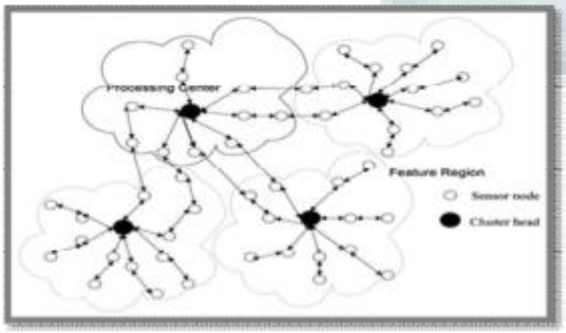

Figure 1: Cluster-based WSN Architecture.

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 malicious nodes. Also, to address the energy consumption, gain in reliability, minimum delay and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements. 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. LITERATURE REVIEW

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, 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. In the context of secure multipath routing for intrusion tolerance, in [10] 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 [11] the authors considered a disjoint multipath routing protocol to tolerate intrusion using multiple disjoint paths in WSNs. The research proposed work also uses multipath routing to tolerate intrusion. However, the work specifically focuses on the amount of energy being consumed for intrusion detection and also to reduced energy consumption in multipath routing to tolerate intrusion. Moreover, the work consider intrusion detection to detect and evict compromised nodes as well as the best rate to invoke intrusion detection so that the energy consumption is reduced considerably along with security and reliability gain to maximize the system lifetime.

In, voting based IDS approach given 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. In general there are two approaches by which energy efficient IDS can be implemented in WSNs. One approach is applicable to flat WSNs where an intermediate node provides a feedback about the maliciousness and energy status of its neighbor 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. Another approach the author adopt in [1] is to use local host-based IDS for energy conservation (with SNs monitoring 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. The solution author 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, the proposed research work extends from [1] with considerations given to explore more extensive malicious attacks, 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" 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. For effective fault tolerance ad hoc on-demand multipath distance vector (AOMDV) [14] is used to achieve reliability and QoS gain with minimum energy consumption.

III. PROPOSED PLAN OF WORK

As Cluster Based Heterogeneous Wireless Sensor Network(HWSN) consists of tiny sensing nodes which are deployed in a remote or hostile region, such as battlefield, it is prone to various types of attacks like jamming, hello flood, selective forwarding, sinkhole, Sybil, packet alteration, bad mouthing etc.. In my observation it is found that existing Intrusion Detection Systems cannot resist to the overall attacks and has some limitations like it has high false positive rate and low detection rate. Also, it cannot detect unknown attacks, which are not in the model base. Hence, it degrades the performance of the system. Also, the Intrusion Detection Systems consume large energy of the sensor node, thus it is necessary to design energy efficient Intrusion Detection Systems and energy efficient multipath routing mechanism to increase the network lifetime. Following are the proposed research plan of work.

- To detect intrusion through packets in the Heterogeneous Wireless Sensor Network and identify it as normal or abnormal packets.
- To identifying the type/nature of the intrusion/attacks by analyzing the abnormal packets.
- To prevent destruction of the system by raising an alarm before the intruder starts to attack.
- To explore more extensive and destructive malicious attacks in HWSN, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks.
- Also, 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.
- To investigate the use of trust/reputation management to strengthen intrusion detection through "weighted voting" leveraging knowledge of trust/reputation of neighbor node.
- Using weighted voting scheme in intrusion detection system (IDS) would considerably reduced the false positives (FPs) and false negatives (FNs) ratio.

IV. RESEARCH METHODOLOGY

In Cluster-Based WSN, due to the heterogeneous nature of SNs, the capability of CH is greater than general SN. Additionally, because CH aggregates sensed data from SNs, it therefore often suffers attack.

The CH used to detect intruders, which not only reduces the consumption of energy, but also efficiently decrease the amount of information in the entire network. The Cluster-Based WSN has following features.

- Self-organization
- Short-range broadcasting communication and multipath routing
- Dense deployment of the sensors
- Frequently changing topology, due to fading and node

failures

- Limitations in computational resources, such as battery power and memory

In the proposed research hierarchical trust management for trust-based intrusion detection architecture is consider through “weighted voting” leveraging knowledge of trust/reputation of neighbor nodes. Voting involves the derivation of an output data object from a collection of n input data objects, as prescribed by the requirements and constraints of a voting algorithm. In data fusion, voting is method of combining different data delivered by several sources (e.g. sensors) whose outputs may be mistaken, delayed, or completely missing. In high reliable systems, voting is required whether the multiple computation channels comprise redundant hardware units, different software modules, identical hardware and software with various data, or any other combination of hardware, program and/or data redundancy.

The main aim of any voting algorithms is to achieve high dependable outputs out of redundant components in order to increase the level of the entire critical-system dependability. Considering this aim, the characteristic/behavior of voting algorithms and the concept associated with theory of each evaluation parameter is one of the proper ways to develop any voting algorithm design methodology. The proposed design approach based on a well understanding of the concept of dependability leads to considerably reduce the false positives (FPs) and false negatives (FNs) ratio. Voting algorithm is considered as a widely used fault masking strategy for increasing the dependability of real-time critical computer systems. The dependability of a voter can clearly affect the whole system performance. Consequently, quantifying the dependability aspects for the results of voting algorithm is a key issue in evaluation voting algorithms.

The proposed design makes use of on-demand multipath protocol called ad hoc on-demand multipath distance vector (AOMDV) specially developed for heterogeneous WSN. AOMDV is based on a prominent and well-studied on-demand single path protocol known as ad hoc on-demand distance vector (AODV). AOMDV extends the AODV protocol to discover multiple paths between the source and the destination in every route discovery. Multiple paths so computed are guaranteed to be loop-free and disjoint. AOMDV has three novel aspects compared to other on-demand multipath protocols. First, it does not have high inter-nodal coordination overheads like some other protocols (e.g., TORA, ROAM). Second, it ensures disjointness of alternate routes via distributed computation without the use of source routing. Finally, AOMDV computes alternate paths with minimal overhead, it does this by exploiting already available alternate path routing information as much as possible.

The research proposes an intrusion framework for information sharing, which utilizes hierarchical architecture to improve intrusion detection capability for all participating nodes. Following are the key concept for intrusion framework.

A. Local Agent

The local agent is responsible for monitoring the information transmitted and received by the sensor. The node maintains an internal database which stores a information about malicious nodes in network. When thenetwork isconfigured, the sensor nodes lack any knowledge about malicious nodes. The signature database is gradually constructed, after the deployment of WSNs. The entry into the malicious node database is created and propagated to everynode by CHs.

B. Global Agent

The global agent is responsible for monitoring the communication of its neighbor nodes. Due to the broadcasting natureofwireless sensor networks, every node can receive all packets within its communication range. We use the monitoring mechanism and pre-defined routing rules with two-hop neighbor knowledge to monitor these packets. If the monitor nodesdiscover anypotential breach ofsecurityin their radio range, they create and send an alert to the CHs. Then, the CHs on receiving the alert, makes the decision about a suspicious node accordingly. Both agents are implemented in the application layer.

C. Evaluation of Alert Packets

The CHs are responsible for alert aggregation and computation. The research proposes four levels of trust, so that it can compute the alert counter for each malicious node, based on trust states of our monitor nodes. The malicious counter defines the threshold value of malicious activities of a sensor node which cannot be exceeded. If the value of the malicious counter of a sensor node exceeds the threshold, the sensor node is revoked from the cluster and WSNs.

1. After deployment, the sensor node builds its direct neighbor node’s list and sends it to the sink node.
2. The sink node finds the set of nodes which corporately cover all nodes in the network as the chosen monitor nodes.
3. The sink node sends the request message to these chosen nodes to require them activating their intrusion detection modules.
4. Every message sent by sensor node or sink node is

authenticated by using their shared keys.

In this section, research works apply hierarchical trust management protocol for trust-based intrusion detection. The propose research first describes the algorithm that can be used by a high-level node such as a CH (or a base station) to perform trust-based intrusion detection of the SNs (or CHs respectively) under its control. Then, research work will develop a statistical method analyzing various parameters to assess trust based IDS false positive and false negative probabilities using weighted voting. Without loss of generality, how a CH performs trust-based intrusion detection on SNs in its cluster will be illustrate. In trust-based intrusion detection, various parameter will be analyze to prolong the lifetime of the network in terms of energy consumption and gain in QoS such as reliability, minimum delay and security.

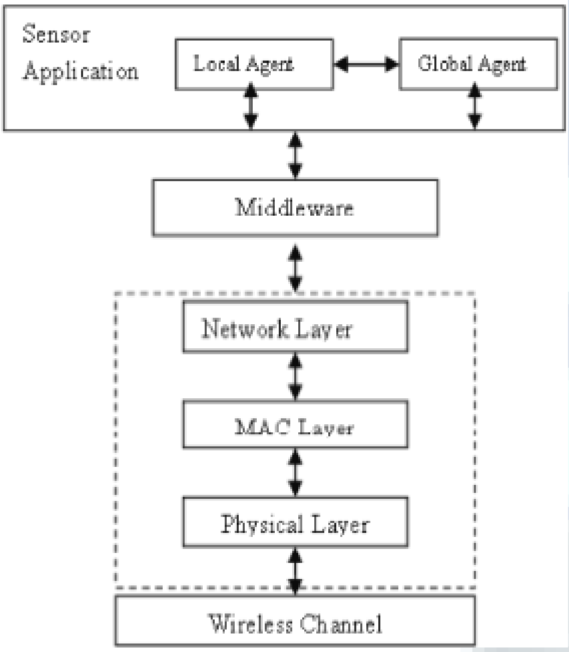

Figure 2: Hierarchical trust management for trust-based intrusion detection architecture

Due to battery depletion or hostile environments (e.g. wind, rain or high temperature) in which WSN may be deployed, sensor nodes are prone to failure. A part of the network can be disconnected and critical data maybe lost because of faults. Thus, fault tolerance is a major concern in wireless sensor networks and even more in critical applications such as healthcare, forest firefighting or nuclear radiation detection where it is not acceptable to lose sensitive data. Fault tolerance is the capacity to keep a network working correctly despite of failures. The Ad-hoc On Demand multipath Distance Vector (AOMDV) routing protocols balance the tradeoff between fault-tolerance and communication overhead. Indeed, increasing the number of paths for a better fault-tolerance. AOMDV is able to cope with route failure due to mobility. In particular, it reduces the packet loss byup to 40% and achieves a remarkable improvement in the end-to-end delay. AOMDV also reduces routing overhead by about 30% by reducing the frequency of route discovery operations, which in turn significantly increase the network resilience and lifetime.

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 and 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 AOMDV routing protocol paradigm for heterogeneous wireless sensor networks will be define and analyzes upon various parameters. 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] Mahesh K. Marina1and Samir R. Das, "Ad hoc on-demand multipath distance vector routing" Wirel. Commun. Mob. Comput. 2006; 6:969–988.

AUTHOR'S PROFILE:

[1]. R.Lohitha, completed B.Tech in Computer Science & Engineering from G.Pullaiah College of Engineering and Technology (affliated to JNTU Ananthapur) in 2012.Currently Pursuing M.Tech in Computer Science and Engineering in Dr.KV Subba Reddy college of engineering for Women,kurnool.

Area of interest : Networking,DBMS

[2]. **B.Mahesh**, Completed M.Tech(CSE) from JNTUA, Anantapur in 2011. Attended 2 International conferences & 1 National Conference.

Area of interest is Network Security and Cloud Computing.