ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Anomaly Detection in Wireless Sensor Network Using Sensing Detection Model

Amol N. Rindhe[1], Sanjay V. Dhopte[2]

ME (IT) Scholar, PRMIT&R, Badnera, SGBAU Amaravati Maharashtra India[1]

Professor (IT) PRMIT&R, Badnera, SGBAU Amaravati Maharashtra India[2]

Abstract: Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a battlefield. The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. Intrusion detection system in wireless sensor network is one of the growing research areas in recent years. Wireless sensor networks (WSN) consist of tiny devices. For this purpose, it is a fundamental issue to characterize the WSN parameters such as node density and sensing range in terms of a desirable detection probability. Many network parameters such as sensing range, transmission range, and node density have to be carefully considered at the network design stage, according to specific applications. In this project, we derive the expected intrusion distance and evaluate the detection probability in different application scenarios.

Keywords: IDS, WSN, Anomaly, Security, Threats, Sensor Network

I. INTRODUCTION

Wireless ad hoc networks (WAHN) are autonomous nodes that communicate with each other in a decentralized manner through multi-hop routing. There are two main types of WAHNs, namely: mobile ad hoc networks (MANET) and wireless sensor networks (WSN). Varieties of potential applications such as environment monitoring, health monitoring, military solution are provided by WSN. Wireless sensor networks consist of some cheap and small devices. As they are generally deployed in unprotected environment, wireless sensor network is vulnerable to various attacks. Therefore, security design is one of the important factors for wireless sensor networks. There are two main techniques for security solution: prevention based and detection based. Prevention based techniques are encryption, authentication etc. Prevention based techniques cannot be applied to the wireless sensor networks because of the limited resources and broadcast medium [1]. Detection technique is to identify the attacks based on the systems behavior. Currently, there are two different kinds detection technique: anomaly based and signature based. In this I will focus only towards the anomaly based detection technique. Most of the WSN researches were based on homogeneous and heterogeneous network. In homogeneous networks, all the sensor nodes have the same capability; on the other hand, sensor nodes may be of varying capabilities in heterogeneous networks. Wireless Networks can reduce the complexity of the existing networks. Mainly it reduces three-fourth of the infrastructure, even though it is not adopted for all the applications, due to security issues. There are enormous works done to solve the security issues. Malicious node detection is one of the most critical security issues in wireless networks.

II. RELATED WORK

An anomaly detection system (ADS) is software designed to detect unwanted attempts at accessing, manipulating, and /or disabling of computer mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and disgruntled employees. ADS cannot directly detect attacks within properly encrypted traffic. An anomaly detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses. Anomaly detection is one of the critical applications in WSNs, and recently, several approaches for intrusion detection in homogeneous WSNs have been presented [3], [10], [11].The focus of these approaches aims at effectively detecting the presence of an intruder. First, it is investigated from the aspect of the network architecture. Kung and Vlah [10] take advantage of a hierarchical tree structure to effectively track the movement of an intruder.Intrusion detection is an important aspect within the broader area of computer security, in particular network security, so an attempt to apply the idea in WSNs makes a lot of sense. However, there are currently only a few studies in this area. Da Silva *et al.* [6] and Onat and Miri [7] propose similar IDS systems, where certain monitor nodes in the network are responsible for monitoring their neighbors, looking for intruders. They listen to messages in their radio range and store in a buffer specific message fields that might be useful to an IDS system running within a sensor node, but no details are given how this system works. In these architectures, there is no collaboration among the monitor nodes. It is concluded from both papers that the buffer size is an important factor that greatly affects the rate of false alarms. More extensive work has been done in intrusion detection for ad hoc networks[15].In such networks, distributed and cooperative IDS architectures are also

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

preferable. Detailed distributed designs, actual detection techniques and their performance have been studied in more depth. While also being ad hoc networks, WSNs are much more resource constrained. We are unaware of any work that has investigated the issue of intrusion detection in a general way for WSNs. In this paper we therefore attempt to move towards that direction, defining the requirements, studying the possible design choices and proposing a specific modular architecture appropriate for IDSs in WSNs. In general, network security solutions can be grouped into two main categories: *prevention* based techniques and *detection* based techniques. Prevention techniques, such as encryption and authentication, are often the first line of defense against attacks. Detection based techniques aim at identifying and excluding the attacker after prevention based techniques fail. Detection techniques are divided into two major categories: *signature* detection and *anomaly* detection. Signature detection techniques match the known attack profiles with the current changes, whereas anomaly detection uses established normal profiles and detects unusual deviations from this *normal behavior*. In this work, we introduce a novel anomaly based intrusion detection method for wireless sensor networks suited to their simple and resource-limited nature. Sensor networks are provisioned to consist of stationary sensor nodes that will provide each sensor with stable neighborhood information. In a distributed fashion, sensor nodes will have the ability to record simple statistics about their neighbors' behavior and detect anomalies in them. The anomalies may present themselves at many different network layers. As long as the implementation is resource-aware, any layer may determine the normal's of layer variables and trigger the intrusion alarms for abnormal deviations.

Wireless Sensor Network:

A wireless sensor network is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The envisaged size of a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust although functioning 'motes' of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth. In Wireless Sensor Networks (WSN), a large number of sensor devices are placed in a designated area. Each sensor unit is equipped with a communication unit and a programmable embedded processor having the capability of sensing, data processing, and communicating with other sensors via radio transceivers. The sensors coordinate with each other to establish a network so that they can monitor the designated geographical area. The collected data will be reported continuously to base. In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The envisaged size of a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust although functioning 'motes' of genuine microscopic dimensions have yet to be created. A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm (several nodes may forward data packets to the base station). With respect to security, there are many tools that are used to ensure security in ID systems. The IDSs are very important tools since they can detect intrusions in networks. Many techniques that are result of research are pertaining to network security in general. They are developed for the nodes that have lot of resources in place. For this reason they can't be directly applied to WSN. That led to further research in the area of WSN for modifying techniques or inventing new ones that are best suited for WSN where nodes are energy constrained. Among the researchers on WSN Zhang and Lee [14] are first in researching on security issues of Ad hoc networks. Their IDS which is distributed in nature works based on the detection techniques of statistical anomaly. This technique assumes much traffic and the time taken for detection of intrusion is high and thus not efficient. The cost of this model can't be afforded by any WSN. At times intruders might be moving and detecting such intruder is also important in WSN. This has attracted research in this domain. When nodes are in transit, the mechanisms and techniques are to be altered. The moving objects, their direction and probability of intrusion, detection etc. are to be considered. Second, the intrusion detection problem has been considered from the constraint of saving network resources. For example, Chao et al. [16] have addressed the issue of tracking a moving intruder by power-conserving operations and sensor collaboration. To achieve this, the authors defined a set of novel metrics for detecting a moving intruder and developed two efficient sleep-awake schemes called PECAS and MESH, to minimize the power consumption. Ren et al. [3] further studied the trade-off between the network detection quality (i.e., how fast the intruder can be detected) and the network lifetime. Therefore, the sensor coverage had to be carefully designed according to the detection probability with respect to specific application requirements. The authors then proposed three wave sensing scheduling protocols to achieve the bounded worst case detection probability. Rather than a static WSN architecture as the above approaches, Liu et al. [17] have modeled the intrusion detection problem in a mobile WSN, where each

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

sensor is capable of moving. The authors have given the optimal strategy for fast detection and shown that mobile WSN improves its detection quality due to the mobility of sensors. In this paper, we address the intrusion detection problem from the other angle. Most of the above efforts consider intrusion detection and its efficiency in terms of the single-sensing model in a homogeneous WSN. Instead of the network architecture and detecting protocol design, we provide a comprehensive theoretical analysis on the intrusion detection in both homogeneous and heterogeneous WSNs [18]. The detection probability is theoretically captured by using underlying network parameters, and thus, our work is of paramount importance for a network planner to design WSNs for intrusion detection applications. To the best of our knowledge, this is the first work that considers the intrusion detection problem in a heterogeneous WSN and provides fundamental analytical results on it. The analytical results indicate the improvement on the detection quality in a heterogeneous WSN, as compared to a homogeneous WSN, either for the single sensing detection or the multiple-sensing detection scenarios.

Furthermore, we have modeled the network connectivity and broadcast reachability in a heterogeneous WSN [19], which serve as the necessary conditions for achieving desirable detection probability.

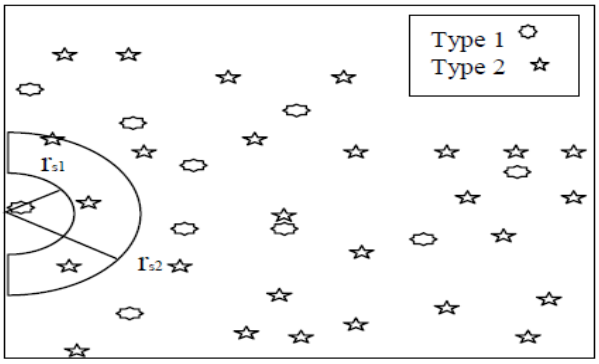

Fig. Anomaly moved area.

A sensor node is a tiny and simple device with limited computational capability and broadcast power. Wireless sensor networks are generally provisioned to consist of a large number of inexpensive nodes reporting their data to a central, more capable sink node using multihop transmission. In general, it is assumed that sensors will be equipped with non-rechargeable batteries and will be left unattended after deployment. However, current and foreseeable future technology have put severe restraints on energy resources of sensor devices. Because long term operation of nodes with limited battery energy is the main design bottleneck of sensor networks, sensor network protocols have to be designed to operate with minimum resource utilization. Security solutions for sensor networks also have to be designed with the limited computational power.

III. ANOMALY STRATEGY MODEL

As illustrated, we consider two intrusion strategies for the movement of the intruder in a WSN. If the intruder (say, a panzer) already knows its destination before entering the network domain, it follows the shortest path to approach the destination. In this case, the intrusion path is a straight line from the entering point to the destination, as illustrated in . The main idea behind this strategy is that the straight movement causes the least risk for the intruder due to the least area that it has to explore by following a straight line toward the destination. The corresponding intrusion detection area S1 is determined by the sensor's sensing range rs and intrusion distance D1. It is because the intruder can be detected within the intrusion distance D1 by any sensor(s) situated within the area of S1. On the contrary, if the intruder does not know its destination, it moves in the network domain in a random fashion. We consider that the intruder tends to minimize the overlapping on its path. Thus, the intrusion path of the intruder can be regarded as a no overlapping curved line, and the intrusion area accordingly is a curved band S2, as illustrated in Fig. In the above two strategies, if the intruder travels the same distance, i.e., *D1=D2*, the corresponding intrusion detection areas approximately satisfy *S1=S2*. Therefore, we adopt a straight path in the following discussion, and the analytical results can be directly applied to the case of the curved path. Furthermore, the intruder can start its intrusion from the network boundary or a random point inside the network domain. For example, the intruder can be dropped from the air and starts from any point in the network domain. There are the detection models to recognize an intruder: single sensing detection model and multiple-sensing detection model. It is said that the intruder is detected under the single-sensing detection model if the intruder can be identified by using the sensing knowledge from one single sensor. On the contrary, in the multiple-sensing detection model, the intruder can only be identified by using cooperative knowledge from at least k sensors (k is defined by specific application requirements).

In order to evaluate the quality of intrusion detection in WSNs, we define three metrics as:

1. Intrusion distance

The intrusion distance, denoted by D, is the distance that the intruder travels before it is detected by a WSN for the first time. Specifically, it is the distance between the point where the intruder enters the WSN and the point where the intruder gets detected by any sensor(s). Following the definition of intrusion distance, the Maximal Intrusion Distance is the maximal distance allowable for the intruder to move before it is detected by the WSN.

2. Detection probability.

The detection probability is defined as the probability that an intruder is detected within a certain intrusion distance (e.g., Maximal Intrusion Distance).

3. Average intrusion distance.

The average intrusion distance is defined as the expected distance that the intruder travels before it is detected by the WSN for the first time.

This analyses the intrusion detection problem in both homogeneous and heterogeneous WSNs by characterizing

intrusion detection probability with respect to the intrusion distance and the network parameters .Two detection models are considered: single-sensing detection and multiple-sensing detection models. The analytical model for intrusion detection allows us to analytically formulate intrusion detection probability within a certain intrusion distance under various application model. This work provides insights in designing homogeneous and heterogeneous wireless sensor network and helps in selecting critical network parameters so as to requirements. The sensing data may have to be reported to the base station, which may be in any location of the network [20]. If the network connectivity is not assured, it is meaningless even the sensor(s) detect the presence of the intruder. Zhang and Hou [21] have proven that in a homogeneous WSN, if the transmission range is equal to or higher than twice of the sensing range, a given coverage probability guarantees a connectivity probability. In this manner, when the coverage is satisfied in the homogeneous WSN, the network connectivity is also statistically guaranteed so that it allows two sensors to communicate with each other. However, in a heterogeneous WSN, the deployment of sensors with different capability complicates the network operation with the asymmetric links. Specifically, a sensor with longer transmission range (i.e., Type I sensor) might reach some sensors with shorter transmission range (i.e., Type II sensors), while the Type II sensors may not be able to reach the Type I sensor. The network connectivity has to be reconsidered. In a heterogeneous WSN, sensors mainly use a broadcast paradigm for communication [12] and high-capacity sensors usually undertake more important tasks (i.e., for broadcasting power management information or synchronization information to all the sensors). This motivates us to examine two fundamental characteristics of a heterogeneous WSN.

IV. CONCLUSION

This system analyses the intrusion detection problem in WSNs by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e. node density, sensing range, and transmission range). The analytical model for intrusion detection allows us to analytically formulate intrusion detection probability within a certain intrusion distance under various application scenarios. Our simulation results verify the correctness of the proposed analytical model. This work provides insights in designing WSNs and helps in selecting critical network parameters so as to meet the application requirements.

REFERENCES

[1] "An Intrusion Detection System for Wireless Sensor Networks" Ilker Onat Ali Miri School of Information Technology and EngineeringUniversity of Ottawa, Canada.

[2] "Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks" Yun Wang, Student Member, IEEE, Xiaodong Wang, Student Member, IEEE, Bin Xie, Senior Member, IEEE, Demin Wang, Student Member, IEEE, and Dharma P. Agrawal, Fellow, IEEE.

[3] S. Ren, Q. Li, H. Wang, X. Chen, and X. Zhang, "Design and Analysis of Sensing Scheduling Algorithms under Partial Coverage for Object Detection in Sensor Networks," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 3, pp. 334-350,Mar. 2007.

[4] S. Banerjee, C. Grosan, A. Abraham, and P. Mahanti,"Intrusion Detection on Sensor Networks Using Emotional Ants," Int'l J. Applied Science and Computations,vol. 12, no. 3, pp. 152-173, 2005.

[5] S. Capkun, M. Hamdi, and J. Hubaux, "GPS-Free Positioning in Mobile Ad-Hoc Networks," Proc. 34th Ann. Hawaii Int'l Conf.System Sciences, Jan. 2001.

[6] A. P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. C.Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet '05). ACM Press, October 2005, pp. 16–23.

[7] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, vol. 3, Montreal, Canada, August 2005, pp. 253–259.

[8] Y. Wang, X. Wang, D. Wang, and D.P. Agrawal, "Localization Algorithm Using Expected Hop Progress in Wireless Sensor Networks," Proc. Third IEEE Int'l Conf.Mobile Ad hoc and Sensor Systems (MASS '06), Oct. 2006.

[9] P. Traynor, R. Kumar, H. Choi, G. Cao, S. Zhu, and T.L. Porta, "Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 6, June 2007.

[10] H. Kung and D. Vlah, "Efficient Location Tracking Using Sensor Networks," Proc. IEEE Wireless Comm. and Networking Conf., vol. 3, pp. 1954-1961, Mar. 2003.

[11] C.-Y. Lin, W.-C. Peng, and Y.-C. Tseng, "Efficient in-Network Moving Object Tracking in Wireless Sensor Networks," IEEE Trans. Mobile Computing, vol. 5, no. 8, pp. 1044-1056, 2006.

[12] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting Heterogeneity in Sensor Networks," Proc. ieee infocom, 2005.

[13] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, vol. 40, no. 8, pp. 102- 14, Aug. 2002

[14] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," IEEE Wireless Communications, vol. 11, no. 1, pp. 48–60, February 2004.

[15] C. Gui and P. Mohapatra, "Power Conservation and Quality of Surveillance in Target Tracking Sensor Networks," Proc. 10th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom '04), pp. 129-143, 2004.

[16] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility Improves Coverage of Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '05), pp. 300-308, 2005.

[17] X. Wang, Y. Yoo, Y. Wang, and D.P. Agrawal, "Impact of Node Density and Sensing Range on Intrusion Detection in Wireless Sensor Networks," Proc. 15th Int'l Conf. Computer Comm. and Networks (ICCCN '06), Oct. 2006.

[18] Y. Wang, X. Wang, D.P. Agrawal, and A.A. Minai, "Impact of Heterogeneity on Coverage and Broadcast Reachability in Wireless Sensor Networks," Proc. 15th Int'l Conf. Computer Comm. and Networks (ICCCN '06), Oct. 2006.

[19] A. Durresi, P.V.K. , S. Iyengar, and R. Kannan, "Optimized Broadcast Protocol for Sensor Networks," IEEE Trans. Computers, vol. 54, no. 8, pp. 1013-1024, Aug. 2005.

[20] H. Zhang and J. Hou, "On Deriving the Upper Bound of for Large Sensor Networks," Proc. Fifth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '04), pp. 121-132, 2004.

BIOGRAPHIES

Mr. Amol N. Rindhe is the student of second year M.E. (Information Technology) of PRMIT&R, Badnera, Amravati – Sant Gadge Baba Amravati University, Amravati, India

Mr. Sanjay V. Dhopte is the Professor (Information Technology) of PRMIT & R, Badnera, Amravati- Sant Gadge Baba Amravati University, Amravati, India.