Abnormal Node Detection in Wireless Sensor Network by Pair Based Approach using IDS Secure Routing Methodology

Khandakar Rashed Ahmed , A.S.M Shihavuddin, Kabir Ahmed, Md. Shirajum Munir and Md Anwar Asad,

Computer Science & Information Technology Department, Islamic University of Technology (IUT), OIC, Bangladesh
Electrical and Electronic Engineering Department, Islamic University of Technology (IUT), OIC, Bangladesh
Department of Computer Science, Dhaka City College, National University, Bangladesh

Summary
Mission critical wireless sensor networks require an efficient, lightweight and flexible intrusion detection methodology to identify abnormal node or malicious attackers. The proposed idea in this paper is to develop a new approach of abnormal node detection in wireless sensor network using IDS security routing methodology by dividing the network into number of pairs. Every node of each pair is responsible to identify abnormality of other node in that particular pair considering different attributes of nodes. The abnormal node detection algorithm uses both signatures and knowledge based routing methodology to achieve most accurate and reliable result.

I. Introduction

Security provisioning is a critical requirement for many sensor network applications (battlefield reconnaissance, homeland security monitoring, etc.). Nevertheless, the constrained capabilities of smart sensors (battery supply, CPU, memory, etc.) and the harsh deployment environment of a sensor network (infrastructure less, unattended, wireless, ad hoc, etc.) make this problem very challenging [1]. Most of the existent works rely on the traditional cryptography and authentication techniques to establish a trustworthy relationship among the collaborative sensors. However, the unreliable wireless channels and unattended operation make it very easy to compromise/capture sensors and break the trust relationship established beforehand. Many different kinds of attacks against wireless sensor networks have been identified so far, e.g., bogus routing and sensed data attack, select forward attack, sinkhole attack, wormhole attack, black hole attack and hello flood attack, etc. [2]

All the security solutions proposed so far can be classified into two main categories: prevention based techniques and detection based techniques. Prevention based techniques, such as encryption and authentication, are often regarded as the first line of defense against attacks. Detection based techniques are designed to identify and isolate attackers after prevention based techniques fail. Furthermore, there are two types of detection based techniques: signature based detection and anomaly based detection. Signature based detection techniques match the known attack profiles with suspicious behaviors whereas anomaly based detection techniques detect unusual deviations from pre-established normal profiles to identify the abnormal behaviors.

In the proposed methodology, a new pair-based abnormal node detection scheme is introduced which is a combination of prevention and detection based techniques. The total network is divided into a number of pairs. A pair is formed using the special algorithm considering different sensor attribute of nodes which produces the initial knowledgebase for the pair as well as for the sensor network group. Many numbers of pairs forms a sensor network group within a small range of area. The knowledgebase developed its own knowledge dynamically using different sensor node behavior and activities. The nodes in a pair have the same sensing capability and are physically close to other node of the pair. Abnormal node detection algorithm is scheduled to run in locally for each pair and centrally for a sensor network group. The method used both knowledge based and signature based techniques of IDS security routing methodology to identify abnormal node in a pair or in a group of wireless sensor network.

II. Background

In this section, some related works in the security field of wireless sensor network is reviewed. An important aspect of the broad area of security is anomaly detection. Many solutions have been proposed to traditional networks [3, 4,], but restrictions of wireless sensor network resources make direct application of those solutions unavailable.

Encryption and authentication are two primary techniques to secure wireless sensor networks against malicious access. The core ideas behind such techniques rely on key management. Li et al. proposed the hexagon-based key pre-distribution scheme that can improve the effectiveness of key management in sensor network by using the bivariate polynomial in a hexagonal coordinate system

Manuscript received December 5, 2008
Manuscript revised December 20, 2008

based on the deployment information about expected locations of the sensor nodes [5]. The key management schemes mentioned belongs to the type of static key management schemes. Another type of key management scheme is kind of dynamic scheme in which keys are updated periodically or on demand as a response to node capture. Moharrum and Eltoweissy compared dynamic key management with static key management and, as the result, proposed an EBS (Exclusion basis system)-based dynamic key management scheme [7]. Eltoweissy et al. proposed a dynamic key management scheme called LOCK LOcalized Combinatorial Keying) which is an EBS-based hierarchical key management scheme that can only be used in hierarchical wireless sensor networks [8].

In [8], an IDS model for ad-hoc networks is presented following the behavioral paradigm. The IDS is decentralized and detection is made by clusters. A technique to safely elect the responsible node for monitoring each cycle was developed. This solution is expensive, thus being in adequate to a wireless sensor network. Doumit et al. proposed a self-organized criticality and stochastic learning based intrusion detection scheme that takes advantage of self organized criticality for a certain location based on an environment variable and uses a Hidden Markov Model to detect future anomalies [9].

Agah et al. proposed a non-cooperative game approach in which the key is to find the most vulnerable node in a sensor network and protect it [10]. Silva et al. defined multiple rules that can be used to determine if a failure has happened and to raise an intrusion alarm if the number of failures exceeds a predefined threshold [16]. A newly proposed scheme, called the insider attacker detection scheme, takes into consideration of multiple attributes simultaneously in node behavior evaluation without the requirement for prior knowledge about normal or malicious sensor activities [11]. It has high accuracy and low false alarm rate when some sensor nodes are misbehaving.

III. Aims and Objectives

The research aim is to provide an efficient technique to detect abnormal node in wireless sensor network using IDS security routing methodology. This is totally a new approach where both IDS techniques of anomaly detection in wireless sensor network are used. Security in wireless sensor network is still an important issue rather than wired network. This research work will turn the less infrastructure wireless sensor network into a trust worthy network for sensor nodes by establishing reliable and secure communication environment.

The objective is to attain lightweight and flexible abnormal node detection algorithm to identify abnormal node in wireless network regardless of limited memory, processing power, battery etc. The development of this new approach of anomaly detection technique in wireless sensor network can give dependable and protected communication among sensor nodes and can control abnormal behavior of nodes in well-organized way than any other approach used before.

IV. Significance and Innovation

Anomaly detection or to some extent abnormal node detection in wireless network is not the same as in the wired network. Techniques geared towards wired networks would not suffice for an environment consisting of multihop wireless links because of the various differences such as lack of fixed infrastructure, mobility, the ease of listening to wireless transmissions, lack of clear separation between normal and abnormal behavior in sensor networks. Considering all options and limitations the proposal is to divide the network into number of pairs and to combine the signature base and the knowledge base routing methodology, which can overcome the barrier in abnormal node detection scheme in wireless sensor network.

The proposed approach is a novel one in the context of abnormal node detection. Following the proposal, the whole network is divided into number of pairs where a pair defines a community between two adjacent nodes. This will reduce the complexity of the methodology to identify the abnormality between nodes in a network. In order to provide more accurate result, signature based routing and knowledgebase abnormal behavior searching technique can be used which is known as Intrusion Detection System (IDS). The total developed platform and structured methodology can detect abnormal node in wireless sensor network in a more reliable and efficient manner.

The proposed system focuses the accurate detection of abnormal node and building the system knowledge based on the nodes behavior considering the wireless network constraint.

V. Proposed Methodology

Pair based abnormal node detection system required to make a sensor network platform where the whole network will be segregated into number of pairs. A pair consists of two member node where they are adjacent to each other. Many pairs constitute wireless sensor network group. Nodes can send and receive message with other node where source and destination location can be within pair,

pair–to-pair or group-to-group. Special algorithm is used for making pairs between adjacent nodes. Predefined attributes of nodes like distance between nodes, energy level, initial request response time etc can drive the algorithm to make decision to form pair in the network. New node, occurred into the network then searches for the single node which wants to make a pair. If there is no single node available then new node will advertise that it wants to make pair. The first pair in the network is considered as the central pair of the group which is responsible for the group controlling and group-to-group communication. Once a pair is formed then each node has the responsibility to detect the abnormality of the other node in that particular pair using the locally and centrally deployed knowledgebase (databases). As a result, one node is completely dedicated to find out the abnormal condition of one node only which will obviously produce more better, accurate and reliable result than other approach.

By dividing the network into many numbers of pairs, naturally it is reducing the problem space and also decreases the complexity of the algorithm. All the IDS security solutions proposed so far can be classified into two main categories: prevention based techniques and detection based techniques [12]. Prevention based techniques, such as encryption and authentication etc. and detection base techniques are designed to identify and isolate attackers after prevention based procedures fail [14][15].

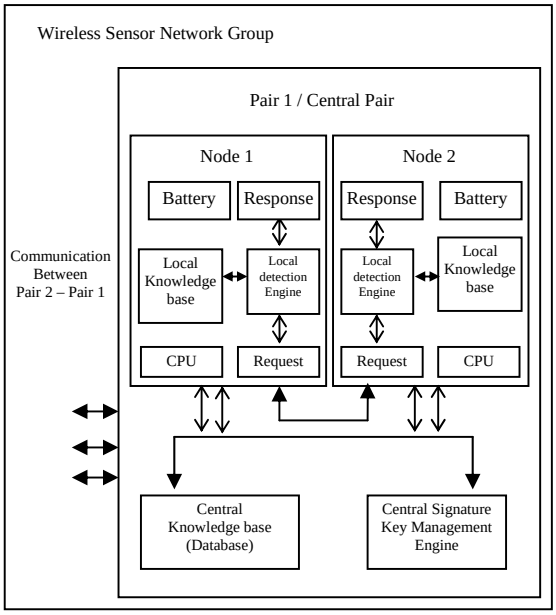

Figure 1: Proposed System Model for Abnormal Node Detection

This system uses two types of detection based approach for detecting abnormal node in wireless sensor network:

First one is Signature based detection. Signature based detection system is deployed for secure communication between pair-to-pair nodes and group-to-group communication. Data exchanged between nodes contains defined packet format. Two types of tag are added to the packet format to make sure the maximum security. One is specific to message ID and other one is system specific DSA/RSA key. The format can be encoded and decoded by those pair only who keeps continuous communication with central engine which is dynamic always. Response and request message between nodes are verified by central key management engine. Central Signature Management key is always communicating with local detection engine for verification and up gradation.

Second one is Anomaly based detection. This approach of detection technique identifies unexpected and abnormal behavior in the network. This is typically a good approach for unknown problems but still it can be prone to false positives [13]. Known behaviors are stacked in the knowledge base and it is used by local detection engine to identify the problem pattern. Local knowledgebase contains the information about the attribute (like distance between them) of the adjacent node. This information is used by the local detection engine to identify the abnormal condition of the adjacent node. Central knowledgebase contains information of every pair in a group and also other group's information. It's always updating the database and sinks with the all local knowledgebase so that all local detection engines can be updated about the anomaly behavior of the group and outside the group. Similarly new findings of local databases also should be updated in central databases. In any test case, local detection engine first consult with local knowledgebase and if fails then contact with Central knowledgebase to identify the problem.

This methodology ensures the development of the most valued knowledgebase to identify abnormal node detection in a wireless sensor network. The more the lifetime of the network, the system can give more accurate result. The final development of the proposed system can fill up the gap to detect abnormal node in wireless sensor network.

VI. Conclusion

WSN pose unique challenges and because of this traditional security threats that all the other wireless network face can not assumed for WSN. The very common threat to wireless sensor network communication is abnormal node detection. The attack is so obvious in

the network that without strong procedure, the total communication can be broken down. The successful development and deployment of the research will enhance the performance of the sensor network. Moreover, different types of wireless sensor network application which was creating problem due to abnormality, may find some new solution with the help of this research. Wireless communication is becoming the main communication medium day by day. Wireless Sensor Network is one of the promising sectors in the wireless communication technology. As the research is related to network architecture, success of this research means some steps forward to the wireless network world and that is directly related to national and international benefit.

Reference:

[1] F. Liu, X. Cheng, F. An, "On the Performance of In-Situ Key Establishment Schemes for Wireless Sensor Networks," in IEEE GLOBECOM 2006, San Francisco, CA, November 27-Decrmber 1, 2006.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Ad Hoc Networks, Vol. 1, No. 2-3, 2003, pp. 293-315.

[3] K. Ilgun, Ustat: A real-time intrusion detection system for unix, in Proc of IEEE Computer Society Symp on Research in Security and Privacity, May 1993.

[4] K. Ilgun, R. A. Kemmerer, and P. Porras, State transition analysis: A rule-based intrusion detection approach, IEEE Trans on Software Engineering, 21 (1995), pp. 181–199.

[5] G. Li, J. He and Y. Fu, "Key management in sensor networks", in Proc. International Conference on Wireless Algorithms, Systems and Applications 2006, August 2006, pp. 457-466.

[6] M. Moharrum and M. Eltoweissy, "A study of static versus dynamic keying schemes in sensor networks", in Proc. 2nd ACM international workshop on performance evaluation of wireless Ad Hoc, sensor, and ubiquitous networks, 2005, pp. 122-129.

[7] M. Moharrum, M. Eltoweissy and R. Mukkamala, "Dynamic key management in sensor networks", IEEE Communications. Vol. 44, No. 4, 2006, pp. 122-130.

[8] Y. an Huang and W. Lee, A cooperative intrusion detection system for ad hoc networks, in Proc of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, 2003, pp. 135–147.

[9] S. Doumit and D.P. Agrawal, "Self-organized criticality & stochastic learning based intrusion detection system for wireless sensor network", in 2003 IEEE Military Communications Conference, Vol. 22, No. 1, 2003, pp. 609-614.

[10] A. Agah, S. Das, K. Basu and M. Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach", in 3rd IEEE International Symposium on Network Computing and Applications, Boston, MA, August 2004, pp. 343-346.

[11] F. Liu, X. Cheng and D. Chen, "Insider Attacker Detection in Wireless Sensor Networks", in 26th IEEE International Conference on Computer Communications, 2007, pp. 1937-1945.

[12]Guorui Li, Jingsha He, Yingfang Fu "A Distributed Intrusion Detection Scheme for Wireless Sensor Networks", 28th International Conference on Distributed Computing Systems (ICDCS).

[13] "Secure Routing and Intrusion Detection in Ad Hoc Networks", 3rd International Conference on Pervasive Computing andCommunications (PerCom 2005), Kauai Island, Hawaii".

[14] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Mobicom 2000.

[15] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks", Mobicom 2000

[16] A. P. da Silva, M. H. Martins, B. P. Rocha, A. A. Loureiro, L. B. Ruiz, H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in ACM Q2SWinet'05, 2005.