A novel anomaly detection algorithm for WSN

Aswathy Balakrishnan
Mtech Student, Department of ECE
MES College of Engineering
Kuttippuram,India
Email: aswathybalakrishnankp@gmail.com

Rino PC
Assistant Professor, Department of ECE
MES College of Engineering
Kuttippuram,India
Email: rinopc@gmail.com

***Abstract*—Wireless sensor networks (WSNs) are gaining more and more interest in the research community due to their unique characteristics and have a lots of interesting applications.Besides energy consumption security of WSN is being a critical issue nowadays.This is because WSNs are easily effected by various types of attacks and node compromises so they require security mechanisms to defend against them.An intrusion detection system (IDS) is one such solution to the problem.There are many research works focused in the area of signature based anomaly based IDS.Based on these malicious activities there is a need of addressing a new or modified versions of IDS algorithm.The proposed algorithm, abbreviated as AD(anomaly detection) algorithm has dedicated procedures for secure cluster formation,periodic re-clustering,and efficient cluster member monitoring and then the detection of different attacks.The performance of AD algorithm in identifying and detecting intrusions using a rule-based anomaly detection scheme is studied via simulations.**

***Keywords*-Wireless sensor networks;Anomaly-based detection;Cluster Head(CH);Cluster Member(CM)**

I. Introduction

Wireless sensor networks (WSNs) have become a latest research topic in recent years.A WSN mainly consist of hundreds or even thousands of small,cheap sensor nodes which can communicate with one another wirelessly and which may be destroyed in a hostile environment. Currently,many of the researches are there on providing security solutions for WSNs.They are mainly focused on key management, authentication,and secure routing,as well as secure services including secure localization and secure aggregation etc.Many of the techniques have been proposed for the security of WSN,but they can only cope with the external attackers. However, strong internal attackers,which managed to penetrate the first perimeter of defense,can only be dealt with using intrusion detection systems (IDSs). Various signature based and anomaly-based IDS architectures have been proposed for WSNs.
In this grouping technique, we make use of the clustering protocol and its operation is to select a set of cluster heads (CHs) among the different nodes in the network and to cluster the rest of the nodes with them.Cluster heads are responsible for the coordination among the nodes inside their clusters (intra cluster data gathering) and for forwarding the collected data to the sink node after efficiently aggregating them.Instead of this, cluster heads are also tasked with intrusion detection functions, such as collecting intrusion alarms from their cluster members (CMs). Additionally, the cluster head nodes may also detect attacks against other cluster head nodes of the network, since they constitute the backbone of the routing structure.Accordingly the present work contributes an anomaly rule based detection for cluster based WSN. The algorithm mainly defines the following concepts.

- It defines a trust-aware leader election metric that makes the leader election process of clustering which is immune to ranging attacks.
- It introduces a monitoring mechanism to monitor both the cluster members and the cluster heads.
- It specifies a rule-based detection engine that accurately analyzes data packets
- It detect signs of sensor network anomalies

The remaining section of the paper is organized as follows. In Section II, existing anomaly detection algorithms developed for cluster-based WSNs are outlined. A detailed description of the anomaly detection algorithm is provided in Section III. Section IV illustrates the obtained simulation results, followed by detailed reports. Finally, conclusions are given in Section V.

II. Related works

In a network or a system, any kind of unauthorized or unapproved activities are called intrusions.An Intrusion Detection System (IDS) is a collection of the tools, methods,and resources used to help identify, assess, and report intrusions.In [1],it introduced the problem of intrusion detection system on WSNs and present an intrusion detection system that fits the demands and restrictions of those networks.It proposed a decentralized IDS model that fits to the WSN restrictions and peculiarities.The proposed algorithm was divided into the following phases: Phase:Data acquisition, Phase 2:Rule application, Phase 3: Intrusion detection.In [2], it proposed a method called Incremental Intrusion Detection System (INIDS),it works as the combination of signature based detection and anomaly based detection. Therefore it also helps to detect data forwarding attacks like selective forwarding attack where nodes transmit only some of the packets received, denial of service attack where node denies transmitting packets to other nodes within range.The issue of anomaly detection in hierarchical, cluster based WSNs has been addressed by several scientific works.According to a recent study,the developed ADSs can be categorized based upon the incorporated anomaly detection pattern. The detection pattern

978-1-4673-6994-7/15 $31.00 © 2015 IEEE
DOI 10.1109/ICACC.2015.29

is basically linked to who takes charge of carrying out the data processing procedure of anomaly detection.First, the cluster head is responsible for the processing and decision making alone.Second, the cluster head and cluster members cooperate to accomplish this.Third,this procedure is carried out by a central authority namely, the base station (BS)[3,4].

From the above analysis it becomes clear that a wide research work has been done in the area of anomaly based detection for cluster-based WSNs. From this viewpoint in this paper, we move towards that direction by proposing a modular, robust, and lightweight trust based ADS architecture specifically designed for this class of cluster based wireless sensor networks.

III. Anomaly detection algorithm for WSN

A. Detailed protocol description

The AD(anomaly detection) algorithm make use of a round-based approach towards cluster formation and anomaly detection. At the end of each round (RP), the network is re-clustered again and new cluster heads are assigned then. A monitoring mechanism is introduced to assist the analysis and decision making process of detecting the anomalies.The proposed algorithm undergoes through various phases.

1) Phase 1: Secure leader election and cluster formation: In [4], an effective and energy-aware self-organizing clustering methodology for UWB sensor networks, named EASOC has been proposed. It presents a clustering algorithm closed to the UWB special characteristics. EASOC has dedicated procedures for energy efficient cluster head selection and periodic re-clustering, where the termination of the clustering process is controlled through different rounds. Simulation based studies demonstrate that the proposed algorithm balances the energy dissipation over the whole network, thus prolonging the network lifetime. This protocol is a leader-first clustering protocol developed for wireless sensor networks having the characteristics of UWB sensor networks. If a node i has Ni neighbors, then its interference factor IFi according to SOC is computed by Eq. (1)

$$IF_i = \frac{1}{N_i} \sum_{k=1}^{N_i} D_{ik}^{\alpha} \tag{1}$$

where n is the path loss exponent of the propagation path and Dik is the distance between node i and its k-th neighbor. But since there arise a need of another protocol ie an energy-aware metric,thus formed Energy-Aware Interference factor $EAIF_i$.It is computed as the ratio of the node's interference factor IF_i and its residual energy E_i^{res} This means that the cluster heads are elected first, based on an energy-aware interference factor (EAIF) shown in Equation (2) and then other nodes join these cluster heads forming a multi-cluster network.

$$EAIF_i = \frac{\frac{1}{N_i} \sum_{k=1}^{N_i} D_{ik}^{\alpha}}{E_i^{res}} \tag{2}$$

But this protocol does not offer any security that we need when electing the cluster heads, because some of the internal attackers that do not follow the protocol semantics can lie about their distance or their residual energy inorder to make themselves elected as cluster heads, thus giving them the chance to launch severe attacks.This difficulty is dealt with by modifying the leader election protocol (LEP). For a secure LEP protocol,there introduced a new leader election metric ie the secure leader election indicator (SLEI).

$$SLEI_i = EAIF_i.W_i = \frac{\frac{1}{N_i} \sum_{k=1}^{N_i} D_{ik}^{\alpha}}{E_i^{res}} \cdot \frac{1}{N_i} \sum_{k=1}^{N_i} \theta ki \tag{3}$$

In rule-based detection, the anomaly detector uses predefined rules to classify the anomalies or normalities. While monitoring the network, these defined rules are selected appropriately and then applied to the data packets that are monitored. If any of the rules have been violated or equivalently any of the rules defining an anomaly are satisfied, an anomaly is declared and an alarm will be raised. An alarm generated by a cluster head indicates that a cluster member is an intruder and needs to be revoked. Similarly, if the independent alarms raised by the monitor nodes of a cluster head satisfy the majority-vote rule, then this cluster head is revoked and a new cluster head, among the cluster members, is elected. Each time an untrustworthy node is revoked (the revocation is indicated by a broadcast alarm message).

Consider a node i with Ni neighbors, its SLEIi is computed as follows,where Dik is the distance between node i and its kth neighbor, α is the path loss exponent, Eresi is the residual energy of node i, Wi is a weight ranging from 0 to 1, and θ ki ϵ [0, 1] is a trust value assigned to node i by its peers. The idea behind this definition is that when all nodes have the same EAIFi, we should select the nodes with the highest weighted trust value, Wi. Nodes that have lower weighted trusts are avoided from becoming cluster heads, even though they may have higher EAIFi (note that the EAIF indicator is upper bounded). Basically, these clustering algorithm follows four steps for dividing the network into clusters and defining the cluster heads as shown in algorithm. Each node floods the network with a table containing its EAIFi value and the trust values θik this node assigns to its closest Nu neighbors. The trust metric is initialized to 1 and is updated every time a node enters the monitoring and trust update phase. Trust updates are based on the trustworthiness of a node. We classify the trustworthiness into three grades: trust, distrust, and uncertain, valued as 1, 0, and 0.5,respectively.Hence, if node i behaves maliciously, the trust values assigned to this node by its monitoring neighbors, θki, will be decreased using a two-step method: from 1 to 0.5 and then to 0. Accordingly, Wi and SLEIi will be decreased.The node with the maximum SLEIi is marked as cluster head, and all its neighbors are removed from the table. This procedure continues until there is no node left to be noticed that is not a cluster head.The cluster heads then forward the

collected data to the BS. When a predefined number of data exchanges is reached, namely RP, the entire procedure starts from the beginning. In each round, the cluster heads will be different from the previous ones.Sometimes ther may be a chance that cluster head can also act as malicious node.Inorder to monitor the cluster head we introduced the monitoring mechanism.

2) Phase 2: monitoring and trust update: The next issue we need to consider is the determination of the nodes having ADS on it ie we need to detect how many nodes are there on duty to detect the misbehaviours.So while monitoring the cluster members,the IDS is activated on cluster heads.After an interval which is equal to monitoring period, a cluster member is judged to be abnormal by its cluster head,and then it is revoked.While doing so, the trust value of the detected malicious node is then updated(reduced) and then sent a alarm message.Cluster heads are monitored by their cluster members.Monitoring the Cluster heads is essential because,if the LEP protocol fails there may be some malicious nodes which is undetected,they do not retain so far.A part of the cluster members are then activated for monitoring and making final decisions on the maliciousness of their CH. During each MP cluster members with the highest SLEIi value within its clusters in succession compose the monitoring team of the CH.If any of the Cluster head is detected as abnormal after the MP then the Cluster head is revoked by the monitoring team.After the identification and revocation of the malicious CH, another cluster head, among the cluster members, is elected.Again recluster the networks and then the node with the new highest SLEIi value in the attacked cluster becomes its cluster head.

3) Phase 3: anomaly detection : Our network-based ADS detects anomalies based on the packets that it monitors. Each node running the ADS stores a data structure for each collected packet. Then, each data structure is evaluated according to the sequence of rules defined in table 1. This means that within ADLU, we employ a trust basis rule-based approach to anomaly detection. Rule-based detection appears to be very attractive in the context of WSNs in the essence that the detection speed and complexity certainly benefits from the absence of an explicit training procedure required

The three phases of the ADLU algorithm are summarized in algorithmic form within Algorithm

- **The AD(anomaly detection) algorithm**

Phase 1: Secure Leader Election and Cluster Formation

for each node i in the network do

Step 1:(exchange a ranging-enabled beacon and calculate its EAIFi indicator)

Step 2: flood the network with the table node- IDi, EAIFi ,θik=1,$\forall$ neighbors k

Step 2: construct a table from the received messages

for each node i in the table run the LEP protocol do

if nodes are left in the table then

Step 3: mark node with the maximum SLEIi as cluster head (CH) & delete its neighbors of this CH from table

for each node left in the table **do**

Step 4: node i joins the closest CH & cluster members (CMs) exchange data with their CH

if Rounds greater than repetition period, RP **then** start from the beginning **(Step 1)**

end for

end if

Phase 2:Monitoring and Trust Update

for each node i in the network **do**

if node i is the CH **then**

start monitoring your CMs

if Trust value $<$ 30%, MP **then**

collect data, update, if necessary, the trust values, θik, and execute **Phase 3**

end if

else select the cluster member nodes with biggest SLEIi values, and start to monitor the CH

if Trust value $<$ 50 % **then**

execute **Phase 2** update, if necessary

if RTT value>higher than successive nodes **then**

execute **Phase 2**, update, if necessary

end if

end for

if RSSIvalue>higher than threshold **then**

execute **Phase 2** update, if necessary

end if

end for

Phase 3: Anomaly Detection

Step 1: Declare the anomaly if rules are satisfied and start node revocation

Table I
RULE DEFINITION

Rule description	Detection metric	Attack detected
When a packet is not forwarded as it should increase a counter When this counter reaches a threshold t after MP rounds, calculate the trust value.	Packet drop rate	Selective forwarding (trust value $<$ 30 %)
If the calculated trust value less than 50 %	Packet drop rate	Blackhole attack
Calculate the RTT value between the nodes[5].If RTT value is than other successive nodes, raise an alarm	Packet delay	Wormhole attack
Calculate the RSSI value of each nodes[6] .If RSSI value is higher than a threshold, raise an alarm	ID change	Sybil attack

IV. PERFORMANCE EVALUATION

We used a custom-developed simulation tool implemented in C++ to evaluate the performance of the ADLU algorithm. Three metrics were used to evaluate the efficiency of the ADLU algorithm. These are as follows:

1) The communication overhead, defined as the ratio of the total communication overhead in a system that incorporates our detection algorithm against a system that does not

2) The percentage reduction in network lifetime, resulting from the incorporation of our detection algorithm
3) The detection accuracy, defined as the ratio of the detected attacks to the total number of detected and undetected attacks

We begin by analyzing the communication overhead of the AD algorithm.To simulate this,we chose a network nodes, and we programmed them to selectively launch one of the attacks depicted in Table 1.With regard to selective forwarding attacks , the attacker was forwarding packets with a probability where trust value=30% and when the trust value is $< 30\%$ and the packet forwarding takes place then we conclude that the attacker is executing selective forwarding attack. When the trust value is $< 50\%$ then it is blackhole attack.For a wormhole attack and sybil attack we are calculating the RSSI as well as the RTT value [5,6] In Fig 1,the curves show that the relative communication overhead increases smoothly as the percentage of malicious nodes increases.Communication overhead will be extremely low when the network contains no malicious nodes.

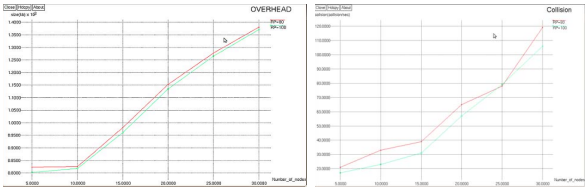

Figure 1. (a) Communication overhead & (b)Reduction in Network lifetime

In Fig 1 (b) illustrates the percentage reduction in network lifetime.Results illustrate that as the percentage of malicious nodes inside the network increases, the reduction in the network lifetime increases.

A. Detection accuracy

The rest of the figures evaluate the detection accuracy of the AD algorithm against the attacks of Table 1.As an overall observation, we can say that the variation of MP solely affects the detection accuracy of the selective forwarding and black hole attacks,sybil attack and wormhole attacks illustrated in below Figures .

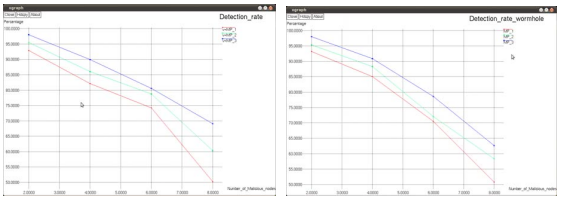

Figure 2. (a) Detection accuracy of blackhole & grayhole attack & (b)Detection accuracy of wormhole attack

V. Conclusion

In this paper, we presented an anomaly detection algorithm specifically designed for cluster-based wireless sensor networks. A novel,trust-aware leader election metric was defined to secure the algorithms cluster formation protocol. The simulation results showed that the proposed algorithm achieves high detection accuracy.In the future, we intend to examine the effectiveness of the AD algorithm in detail by considering larger networks as well as the presence of malicious nodes heavily interfering with the networks

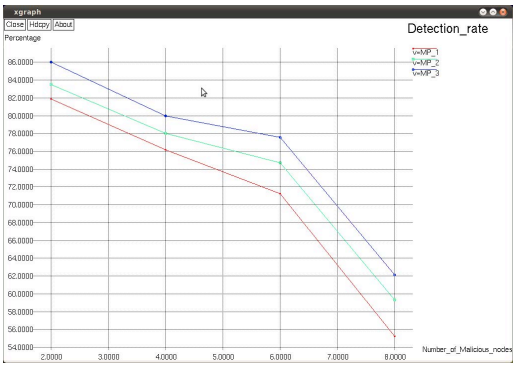

Figure 3. (a) Detection accuracy of sybil attack

References

[1] S.Rajasegarar, C. Leckie, M.Palaniswami and J.Bezdek *Distributed anomaly detection in wireless sensor networks*, 10th IEEE international conference on communication systems (ICCS), pp. 15, 2006.

[2] Priyanka,Shah,Athul and Patel,*Incremental Intrusion Detection System for Wireless Sensor Networks*, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol 2, 2013.

[3] I.M.Atakli, H.Hu,Y.Chen, W.S.Ku and Z.Su *Malicious node detection in wireless sensor networks using weighted trust evaluation*, Spring sim conference, pp 836 to 843, 2008.

[4] C.C. Su, K.M.Chang,Y.H.Kuo and M.F. Horng *The new intrusion prevention detection approaches for clustering-based sensor networks*, WCNC,2005.

[5] G.Koltsidas, E.Karapistoli,and F.N. Pavlidou *An energy-aware self-organizing clustering algorithm for UWB wireless sensor networks* IEEE 19th international conference (PIMRC), pp. 15,sep 2008

[6] Zaw Tun, Aung Htein,Maw *Wormhole Attack Detection in Wireless Sensor Networks* World Academy of Science, Engineering and Technology,2008

[7] Sohail Abbas, Madjid Merabti,David Llewellyn-Jones and Kashif Kifayat *Lightweight Sybil Attack Detection in MANETs* IEEE systems journal, Vol. 7,June 2013