ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.7, 5019–5029
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.7.67 Spec. Iss. on AMABDA-2020

AN EFFICIENT KNOWLEDGE BASED INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORKS

J. RATHIKA[1], M. SORANAMAGESWARI, AND K.H. VANI

ABSTRACT. Wireless sensor networks (WSNs) have a big potential to be applied in crucial situations such as military as well as commercial programs. However, these types of applications are needed often to become deployed within hostile conditions, where systems and conversation are appealing targets in order to attackers. Can make WSNs susceptible to a variety of possible attacks. Because of their characteristics, traditional security systems are not relevant. In this circumstance, we recommend an invasion detection platform for a cluster-based WSN (CWSN) by using Byzantine algorithm, which aims to mix the advantage of abnormality and signature detection that are high recognition rate and also low fake positive, correspondingly. In Furthermore Data Forwarding using Knowledge-based IDS (KB-IDS) in a bunch based WSN; we suggest a technique with regard to securing clients by keeping an archive of various actions of systems inside the system. The proposed work utilizes a Byzantine condition for checking and coordinated effort of the client's neighborhood to improve the security from the system through perceiving attacks. The CHs can similarly get educational data about the malignance of intruder center points by utilizing their enlistment engines.

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 93E10, 68M10.

Key words and phrases. Knowledge-based IDS, WSN, Byzantine Algorithm, CH (Cluster Head).

1. INTRODUCTION

The introduction of multifunctional sensors with cheap and low-power has been driving the significant regarding Wireless Sensor Networks (WSNs). These detectors can be very helpful for many army and business applications to gather and procedure the related information [3]. These programs are required frequently to be used in aggressive environments, wherever nodes as well as communication tend to be attractive focuses on to assailants. In this circumstance, many experts focused on protection issues with regard to wireless sensor networks [5, 7]. Consequently, two types associated with techniques happen to be used: cryptographic techniques and also Intrusion Recognition Systems (IDS) [6]. The primary some shortcoming of this methodology is the failure so as to distinguish absolutely inner assault s when the aggressor knows the genuine keys notwithstanding use them to have the option to encrypt plus decrypt the specific correspondence interchanges [1].

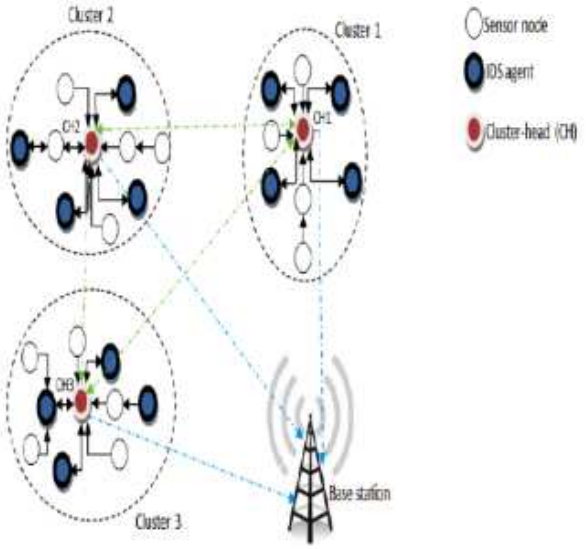

FIGURE 1. Clustered WSN Topology

However, the IDS are used to safeguard the system against each internal and even external attack. The task of the method is to assess a focus on node together with trigger a good alarm whenever suspicious actions occur [8]. Additionally, each IDS agent screens its IDS neighbors even though even the IDS

node might be malicious. These types of agents get data via promiscuous hearing or simply by using a multi-hop conversation mode because illustrated within Figure 1.

2. OUR SYSTEM MODEL

The actual centralized character of cluster-based networks, it really is more achievable to monitor the actual routes as well as traffic. Such networks, the particular nodes tend to be grouped in to clusters so that each team is given the monitor computer known as typically the cluster mind (CH). CHs connect the camp station, systems inside their groupings and other CHs through immediate or oblique routes. Often the network is actually divided into groups in such a way that every cluster has a CH. The CH monitors the behavior of all the member clients inside it is cluster. The particular behavioral information is documented in the form of distinctive events.

2.1. **Network Topology.** The topology of WSN we think about is a cluster-based network, depending on which any two-tier hierarchical trust system is submitted. The people of the WSN are classified into bunch heads (CHs), Intermediate Nodes (INs) and also base station (BS), because shown within Figure 2. In a group, a CH possesses much more energy compared to INs, and INs might communicate with CH directly, while a CH could ahead the blend data to some BS straight or via other CHs. Figure 2 denotes the 0-49 Node are created successfully and the base station as 0 in rounded as red circle.

2.2. **States and Transitions.** Sensor nodes within WSNs have been in different says to conserve power, and it is not essential for all systems to appear to become active constantly due to the limitation of sources. The declares of clients are considered such as hibernation, checking and energetic, which are three basic as well as necessary claims, and other expresses are not taken into account here.

2.3. **Data Transmission.** Identifiers convey the focusing on information ceaselessly at a pre-characterized rate in the persistent style, and it is visit in WSNs, as is sending information with a foreordained timeframe, the component of which can be consistency just as periodicity.

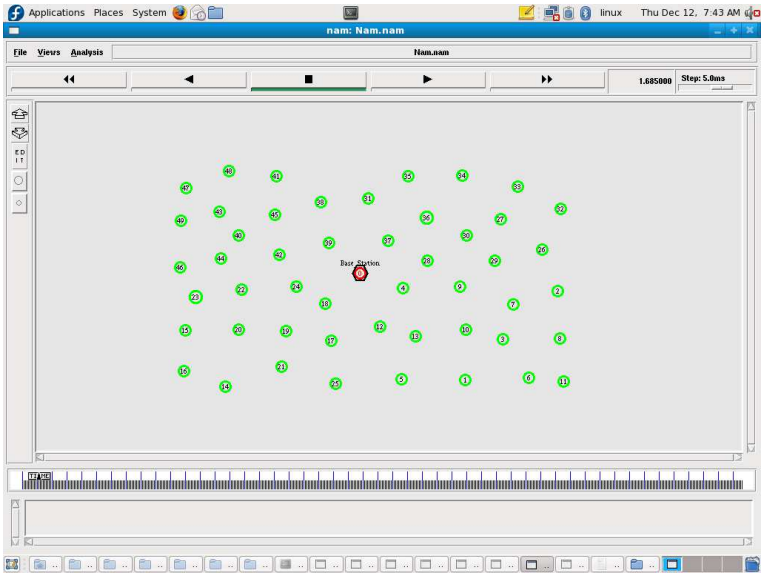

FIGURE 2. Node Creation

- The exact WSN is actually cluster-based, and also INs in a very cluster can communicate with the actual CH immediately, whereas CHs communicate with BSs directly or indirectly by means of other CHs.
- Each and every IN (Intermediate Node) includes a unique ID and is a unique group and CHs having more vitality than in das.
- Your data transmission product in a WSN is cross, including ongoing and event-driven.
- The very states with INs contain hibernation, overseeing and lively, and the change between watching and dynamic is considered during the rely on evaluation for INs.
- Sensor clients are started densely along with redundantly regarding reliability.

Figure 3 denotes the 10, 20, 30, 40 Nodes are assigned as Cluster Head (CH) for the Base station. Figure 4 demonstrates the empty/dummy data forwarded to all the nodes, because some nodes are in sleep stage. So the data forwarded to a node means the Node has been activated.

2.4. **Trust of INs.** Content material trust might be the trust appraisal dependent on watching information, that is information arranged have confidence in

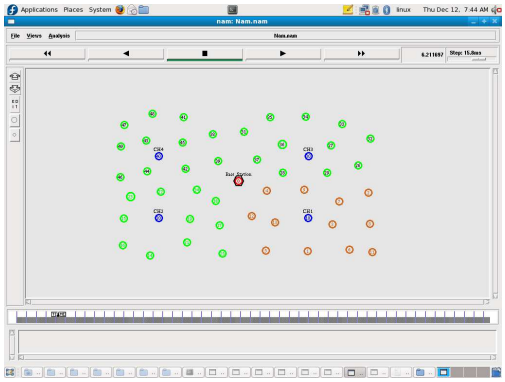

FIGURE 3. Base station assigned as a Cluster Head

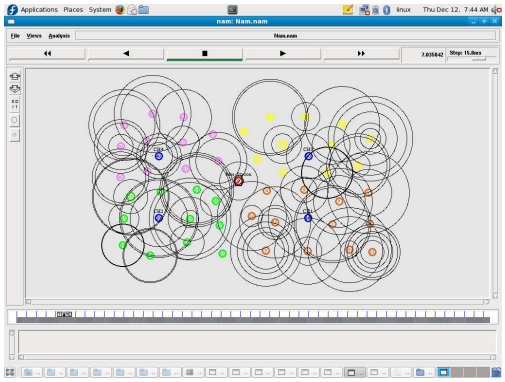

FIGURE 4. Dummy data forwarding

determined through CH. Articles trust is really presented since the WSN is actually an information driven framework and the seeing information would be the factor contrasted with most worry as to applications.

2.5. **Cluster Heads Trust Evaluation.** Cluster heads believe in evaluation is actually enforced within this work through CH-to-CH assessment, BS-to-CH analysis and suggestions from 1-hop neighbors associated with CH to prevent malicious CHs in WSNs. Similar to the rely on of Inches, CH have confidence in evaluation also contains interactive confidence, honesty have faith in and content material trust [10].

2.6. **Intrusion Detection at CH level.** The actual intrusion recognition at CH level is actually conducted through BS w, reducing the potential of being fooled by CHs and reducing the energy usage of CHs. The particular trust computation of each CH is different through IN because there is no state changeover of CHs in this function. Figure 5 denotes the Data requesting from base station to Cluster Head. The Red circles are denoted as the malicious node.

2.7. **KB-IDS IN CLUSTER-BASED WSNS.** Inside our work, KB-IDS, the framework is separated into groups with the goal that each pack is given the CH. Each event comprises of a decent ID, utilize time, kind, attack-ID just as source and furthermore goal IDs of frameworks. Excess episodes and those which were brought about by a couple of system issue and not through gatecrashers will in

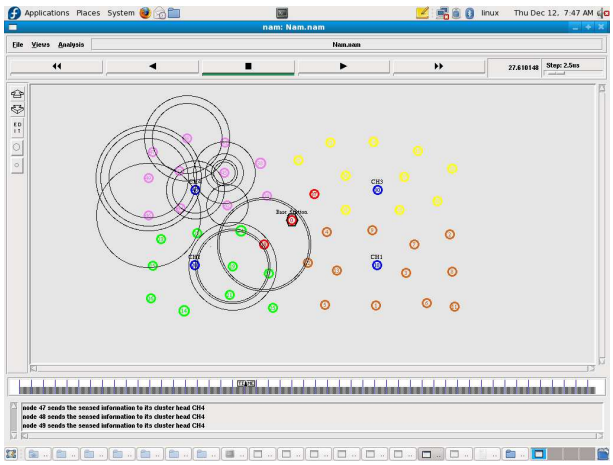

FIGURE 5. Data requesting from base station (in red malicious Node)

general be wiped out through the base station:

$$Ei = [Ty; t; Attack_I D; Source_I D; Dest_D],$$

where Ty is the type of event generated at the time t and i is the event ID from 1 to n.

3. ALGORITHMS

3.1. **Algorithm 1: Byzantine algorithm.** Byzantine Agreement with f = 1.

1: Code for node u, with input value x:

Round 1

2: Send tuple(u, x) to all other nodes

3: Receive tuple(v, y) from all other nodes v

4: Store all received tuple(v, y) in a set S_u

Round 2

5: Send set S_u to all other nodes

6: Receive sets S_v from all nodes v

7: T = set of tuple(v,y) seen in at least two sets S_v, including own S_u

8: Let $tuple(v, y) \in T$ be the tuple with the smallest value y

9: Decide on value y

Byzantine nodes might not follow the process and deliver syntactically wrong messages. This kind of messages may be easily detected as well as discarded.

It really is worse in case byzantine systems send syntactically correct communications, but with the bogus content material, i.e., the gadget guy they send out different information to different clients. Recall that people assumed which nodes are unable to forget their own source tackle; thus, in case a node gets tulle (v, y) in event 1, it really is guaranteed this message had been sent through v.

3.2. **Algorithm 2: Byzantine Agreement.**

1: $x_i \in 0, 1$ - input bit
2: r = 1 - round
3: decided = false
4: Broadcast propose(xi,r)
5: repeat
6: Wait until n - f propose messages of current round r arrived
7: if at least n - 2f propose messages contain the same value x then
8: $x_i = x$, decided = true
9: else if at least n-4f propose messages contain the same value x then
10: $x_i = x$
11: else
12: choose x_i randomly, with $Pr[x_i = 0] = Pr[x_i = 1] = 1/2$
13: end if
14: r = r + 1
15: Broadcast propose(x_i, r)
16: until decided (see Line 8)
17: decision = x_i

General evidence without the limitation to decide for your minimum worth exists too. So far almost all our byzantine agreement codes assume the actual synchronous product.

4. RESULTS AND DISCUSSION

The work has been simulated in NS 2 Simulator under the Linux operating system. A wireless network of 50 nodes, divided into 4 clusters and 1 base station is created. In this section, we evaluate the performances of our intrusion detection framework. First, we evaluate our IDS framework only under KB_IDS.

Second, we combine both techniques (With_KB_IDS, Without_KB_IDS). The Results are compared with Broadcast, Density, Throughput, Delivery Ratio, and Communication Overhead.

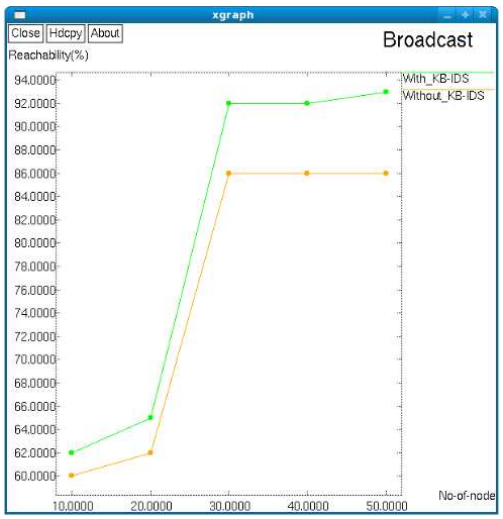

FIGURE 6. Comparison on Broadcast

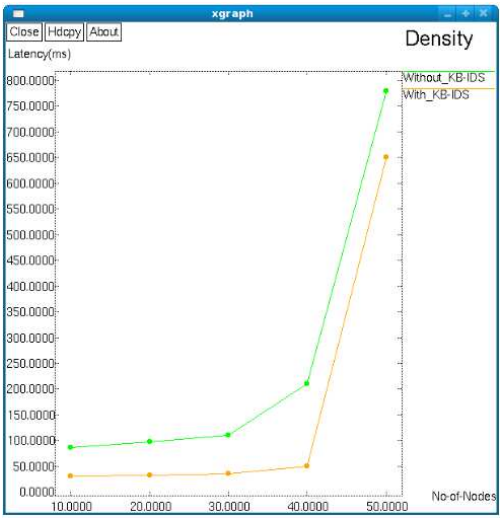

FIGURE 7. Density Comparison Chart

Figure 6 shows the Comparison on the broadcast as With_KB_IDS, Without_KB_IDS. In X_axis denotes the No of nodes and Y_axis denote the Reachablity in Percentage. Figure 7 Shows the Density Comparison chart for With_KB_IDS and Without_KB_IDS. In X_axis denotes the No of Nodes and Y_axis denote the Latency in milliseconds.

Figure 8 denotes the Throughput Comparison chart for With_KB_IDS and Without_KB_IDS. In X_axis denotes the No of packets x 10^3 and Y_axis denote the Throughput x 10^3. In Figure 9 shows the Delivery Ratio comparison chart for With_KB_IDS and Without_KB_IDS. In X_axis denotes the Security Level and Y_axis denote the Delivery Ratio. Figure 10 displays the Communication Overhead compared by With_KB_IDS and Without_KB_IDS. In X_axis denotes the Number of packets x 103 and Y_axis denotes the Overhead.

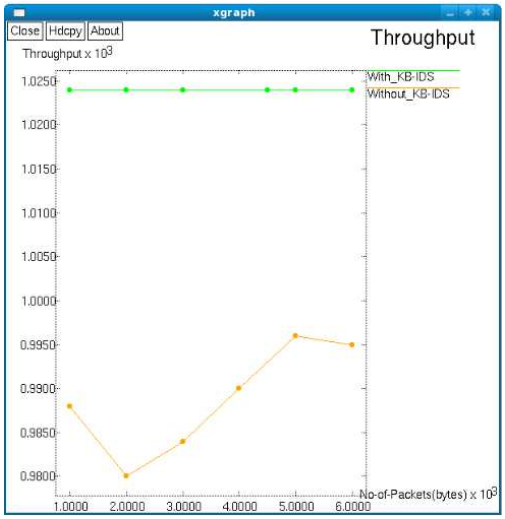

FIGURE 8. Throughput Comparison

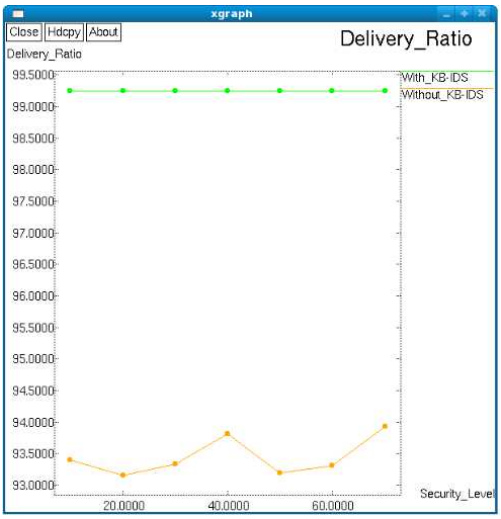

FIGURE 9. Comparison Chart for Delivery Ratio

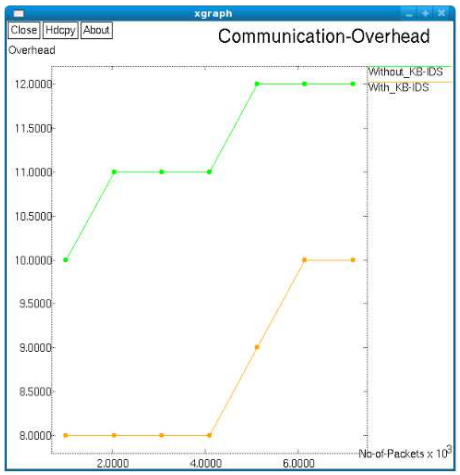

FIGURE 10. Comparison chart for Communication Overhead

CONCLUSION

We proposed a distributed intrusion detection system for cluster-based WSN. The detection structure uses a KB_IDS using Byzantine algorithm. The particular Knowledge-based IDS (KB-IDS) inside a clusterbased WSN and for acquiring nodes by maintaining a record of varied behaviors with nodes in the network.

In the course of trust analysis, factors for communication, multidimensional observing info and express transitions about INs are believed. Malicious behavior nodes may be detected using the trust along with dynamic limit, which increases the flexibility of the method. The KB-IDS showed realistically acceptable simulation results are likened with_KB_IDS in addition to without_KB_IDS just like throughput, density, communication overhead. In future, this approach can be extended with Artificial or Computational Intelligence algorithms to give improved results.

REFERENCES

[1] H. SEDJELMACI, S.M. SENOUCI, M. FEHAM: *Intrusion detection framework of cluster-based wireless sensor network*, IEEE Symposium on Computers and Communications (ISCC), Cappadocia, 2012, 857-861. doi: 10.1109/ISCC.2012.6249409

[2] A. MEHMOOD, S. KHAN, B. SHAMS, J. LLORET: *Energy-efficient multi-level and distance-aware clustering mechanism for WSNs*, Int. J. Commun. Syst., **28**(5) (2015), 972-989.

[3] A. MEHMOOD, J. LLORET, S. SENDRA: *A secure and low-energy zonebased wireless sensor networks routing protocol for pollution monitoring*, Wireless Commun. Mobile Comput., **16**(17) (2016), 2869-2883.

[4] A. MEHMOOD, M.M. UMAR, H. SONG: *ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks*, Ad Hoc Netw., **55** (2017), 97-106.

[5] V. PATEL, J. GHEEWALA: *An efficient session key management scheme for cluster based wireless sensor networks*, IEEE International Advance Computing Conference (IACC), Banglore, 2015, 963-967. doi: 10.1109/IADCC.2015.7154847

[6] T. BASS: *Multisensor data fusion for next generation distributed intrusion detection systems*, in Proc. Net. Symp. Draft, 1999, 24-27.

[7] A. WAHID, P. KUMAR: *A survey on attacks, challenges and security mechanisms in wireless sensor network*, Int. J. Innov. Res. Sci. Technol., **1**(8) (2015), 189-196.

[8] K. VENGATESAN, A. KUMAR, R. NAIK, D. K. VERMA: *Anomaly Based Novel Intrusion Detection System For Network Traffic Reduction*, 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, India, 2018, 688-690. doi: 10.1109/I-SMAC.2018.8653735.

[9] Y.-Y. ZHANG, X.-Z. LI, Y.-A. LIU: *The detection and defence of DoS attack for wireless sensor network*, J. China Univ. Posts Telecommun., **19** (2012), 52-56.

[10] Z. ZHANG, H. ZHU, S. LUO, Y. XIN, X. LIU, X.: *Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks*, IEEE Access, **5** (2017), 12088-12102. doi: 10.1109/ACCESS.2017.2717387.

DEPARTMENT OF DATA SCIENCE,
COIMBATORE INSTITUTE OF TECHNOLOGY,
COIMBATORE
Email address: jradhika@cit.edu.in

DEPARTMENT OF INFORMATION TECHNOLOGY,
GOVERNMENT ARTS COLLEGE,
COIMBATORE
Email address: swarnakannappan@rediff.com

DEPARTMENT OF DATA SCIENCE,
COIMBATORE INSTITUTE OF TECHNOLOGY,
COIMBATORE
Email address: khvani@cit.edu.in