International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Intrusion Detection System in Wireless Sensor Networks by using Lesser Algorithm

Maheswarareddy Annareddy, K.K. Saini

Abstract*: Wireless sensor networks (WSNs) are vulnerable to various types of security threats that may degrade the performance of the entire network. This problem could not provide protection for the attacks on key management and authentication protocols during fatal issues such as service denial attacks, routing attacks, sybil attacks and few other. Over the last few years, researchers have developed different distributed and centralized intrusion detection systems for wireless sensor networks but not reached to a higher performance level. A solution to this problem is the proposed Intrusion Detection System (IDS) with an implementation of more efficient algorithms that can perform routing decisions at every node. There are a couple of routing algorithms in the wireless sensor network which use topology data and takes routing decisions instantly. Extensions to the original position-based algorithm were subsequently presented to perform even more efficiently in conditions where they do not operate. Host growth brings about a route transition, which causes some network to settle on new routes. For ad hoc networks certain routing protocols have already been proposed. The fundamental idea is to allow cellular beneficiaries with bad channel conditions to use the ad hoc network to connect to those cellular collectors who experience great cellular channel conditions. The proposed system can also analyze the network by collecting enough data and detects irregular sensor node(s) behaviour. Finally, the current article explains the implementation of the lower algorithm in sensor networks for evaluating the network intrusion detection system.

Keywords* : Authentication Protocols, Denial of Service, Key Management Protocols, Wireless Sensor Networks.

I. INTRODUCTION

Sensor networks with wireless connectivity is an important field increasingly of research with its wide scope of applications in the real-time scenario. Some of such crucial fields includes critical military monitoring, home security and fire surveillance, and health care. A WSN consists of many independent sensor nodes that are spread in various required areas to collect needed data and transmit the same wirelessly towards more secure node called the sink node or base station node. The data is distinct from the WSN protocols transmitted over the network. Hence, it is important to protect WSN from various security threats.

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
FMaheswarareddy Annareddy*, Department of ECE, Sunrise University, Alwar, Rajasthan, India. Email: a.maheswarreddy@gmail.com
Prof. (Dr.) K.K. Saini, Department of ECE, Sunrise University, Alwar, Rajasthan, India.

Unfortunately, achieving this goal is becoming a major challenge because of WSN's limited resources including battery power, memory, and processing capabilities. Such restricting characteristics do not always make these networks appropriate for conventional safety measures such as cryptography. Because of its open and distributed existence, WSNs are highly vulnerable to attacks, and limited resources for sensor nodes. Additionally, sensor nodes in the transmitted packets of WSN can be distributed randomly in a region to allow easy insertion of an attacker adversary into a WSN. An intruder can compromise a sensor node can inject false messages, change data validity, and discard network primary resources. Denial of Service (DoS) attack is especially considered as one at most common and dangerous attacks which threaten the security of WSN. The attack has various facets and its objective is to disrupt or terminate WSN services. Because security threats cannot always be avoided or prevented, an IDS is required to alert by detecting sensor nodes about identified and unidentified attacks. IDS help track odd or abnormal actions and causes an alarm when an intrusion happens. Implementing WSN IDSs is difficult when compared with other systems due to usual, sensor nodes are built to be small and inexpensive, lacking sufficient hardware resources.

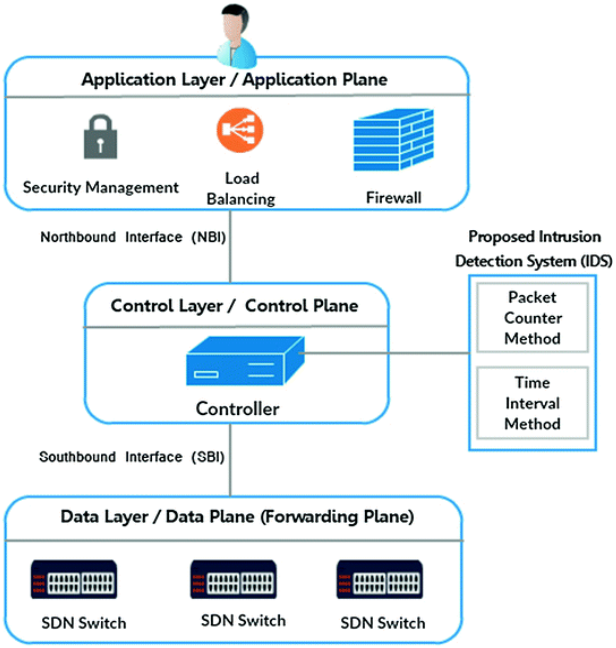

Fig 1. Proposed IDS System for WSN

In addition, no specialized data set containing regular profiles and WSN attacks can be utilized to detect a signature of an attacker.

With the above difficulties, there are primarily two requirements when developing IDS for wireless communication sensors.

The IDS must be highly accurate in detecting an intruder that involves unpredictable attacks, and it must be lightweight in order to ensure minimal overhead on WSN infrastructure. Inspired by the failures of the existing detection systems, this paper proposes a WSN-based intrusion detection model based on the lesser algorithm (LA).

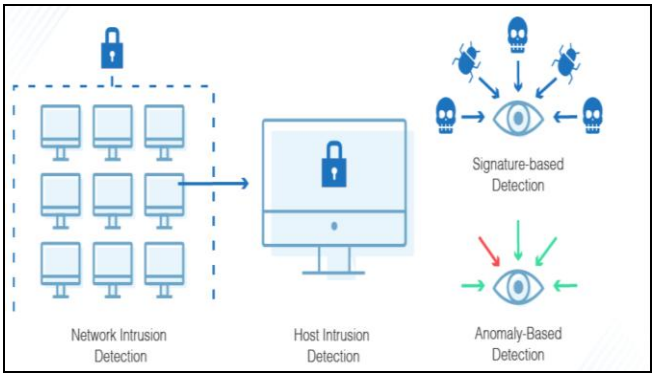

Fig 2. Architecture of IDS followed during the study

II. LITERATURE REVIEW

Securing the sensor network based on trust schemes are successful ways to support WSN against threats and vulnerabilities to protection. Several past researches are done to protect the network with confidence-based models [1]. Models based on trust are mostly based on fuzzy probability, statistical, weighting methods and other models. The systems focus on the method of statistics which uses an average deviation and confidence metrics to detect row attack. In [2], the authors used the principle of fuzzy theory in the network to assess the degree of trust. It is suggested an algorithm for trust evaluation (NBBTE), based on the theory of banding beliefs. In this scheme, a node determines the neighboring node trust value using directional and non-directional trust with on numerous confidence factors. Later, the model identifies the trust value level of every neighboring node. Then, D S proof theory is used to quantify the trust values to find a node's final trust. The model proposed a trust to protect using the fuzzy and proof model. Set theory is used to assess the confidence sensors level and proof theory is used to quantify the confidence value. The author [2] suggested a WSN trust model in which the sensor confidence recommendations are assessed using a fuzzy algorithm. In [3] the authors used probability distribution method to calculate the trust value of a sensor node. In [6], the writers used the confidence measurement and assessment system of weighing. The study [4] used both direct and indirect trust to measure a sensor node in WSN for confidence. The direct confidence measurements require belief in data resources and its communication. The Indirect Trust Calculation (ITC) requires the neighbor node suggestions for the node being monitored. Measured the weighing of a node's misbehavior to identify malicious nodes within the network [5]. A confidence model for WSN with respect to weighting parameters and statistical methods with decreased rate of false-positive is proposed. A model for clustered WSN, based on the cloud model is suggested [6]. A trust-oriented IDS recognition using successful and confident deliveries is proposed in [7]. In this process, a node's trust factor is calculated with Kalman filter. In [8], a physical layer IDS to offer physical layer protection is proposed. This system detects the denial of service attack only because of a jamming attack. At MAC and network layers there is a lack of stability. From the above literature, it is found that it is very important to choose proper confidence metrics to measure an SN's trust. Thus, in order to build an IDS, the nodes ' actions must be definitely considered. In this work we selected the correct confidence metrics for calculating the trust for each layer and detected a node's actions according to the attack. Only few studies are available in this field to develop a trust-based IDS protocol layer, to the best of our knowledge. In this paper the trust is determined by considering the variance of confidence metrics at each point. Next, a sensor node's overall trustworthiness is calculated by combining the individual confidence values.

III. LESSER ALGORITHM

In the LESSAR algorithm a global time in wireless sensor networks is maintained by organizing the entire network system into levels. Level discovery is initially performed upon deployment of the network. Sink that collects information forms the root from all nodes and is assigned level 0. It narrowly casts its neighbors with level discovery packets. Nodes that receive the packets are assigned level 1 and the level discovery packet is broadcast to other nodes. As a result, one node may receive many packets, but it only accepts the one with the lowest level as its ancestor or takes as its own level the value of + 1. Thus, it continues broadcasting. In this hierarchical Network topology, all the sensor nodes are connected. When a new node joins, the level request packet is transmitted to inquire into the current level value so it matches neighbors. From the answers it has received, it elects the smallest one +1 As its level. On node failure, their kids note this when their observation timer expires to keep the message alive. These broad cast level request packets of these nodes and redo the level discovery process. This algorithm may be expanded to provide a set of finite regions with related coverage.

Algorithm #1: Implementation of Lesser Algorithm (Level 1)

Step 1: [Start Initializing]
Step 2: Let *e* be the leaf of Euclidean low-cost spanning tree of any point where *candidateSet*={*e*}
Step 3: [Start deploying the Sensors]
Step 4: while(*candidateSet* !=0)
{ From candidateSet remove a point *p*
Deploy sensor at point *p*
Release from *candidateSet* the points covered by any sensor at any point *p*
At each point of *p* add *candidateSet* by ignoring the vertices *q* of the spanning tree *T* with conditions
(i) From *p*, *r* is the distance for *q* vertex
(ii) No deployed sensors cover *q*

(iii) Should cover the spanning tree path form *e* to *q* for placed sensors}

Step 5: [Stop the procedure]

Algorithm #1: Implementation of Lesser Algorithm (Level 2)

Step 1: [Extension to Step 2 of Level 1]

Step 2: [Establish Internal Neighborhood Graph]

Identification *id* and location *l* is broadcasts for each sensor

Every sensor *e* complies *L(s)* of all *id* and locations *l* that it hears

Let *A(e)*, the nearest list for *e*, with all sensors $a \in L(e)$ so that no $b \in L(e)$ at the interaction region of $|ea|$ circles concentrated at *e* and *a*

For every $a \in A(e)$, with edge weight *(e,a)* is $|ea|/2$.

Step 3: [Establish Reliable support path]

Let the path length be maximum edge weight

Let *x* and *y* be the closest sensor to points from *u* to *v*.

Execute Distributed Bellman-Ford Algorithm for shortest path identification for path *P(x,y)* in the internal neighborhood graph from *x* to *y*.

(u,x), P(x,y), (y,v) is the best path from *u* to *v* with weights of *(u,x)* is $|ux|$ and *(y,v)* is $|ye|$.

SW(u,v) is the maximum edge weights for the best suitable path.

IV. DISCUSSIONS

A system for detecting network intrusion is not limited to inspect incoming traffic only. There are also some patterns and intrusion outgoing from the local traffic. Few attacks could also come inside of the network being controlled just like the trusted host attack. A string-matching algorithm has the scope to implement at every modern detection system. The intrusion detection system introduces the string-matching algorithm to compare the network packet's payload and/or flow against the detection rules pattern entries that are part of a network with a detection system.

V. CONCLUSION

There are a couple of routing algorithms in the wireless sensor network which use topology data for routing decision-making at each node. Extensions to the original position-based routing algorithm were subsequently presented to work even more efficiently in conditions where they currently do not operate. Host growth brings about a route transition, which causes some network to settle on new routes. For ad hoc networks some routing protocols have already been proposed. The essential idea is to allow cellular beneficiaries with poor channel conditions to use and connect the ad hoc network to those cellular collectors encountered with great channel conditions. The current article then describes the implementation of the LESSAR algorithm in wireless sensor networks for analyzing the network intrusion detection system.

REFERENCES

1. E.P.K. Gilbert, B. Kaliaperumal, E.B. Raj singh, and M.Lydia, "Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks," *Computers & Electrical Engineering*, vol. 72, 2018, pp. 894–909.
2. N.Shao, Z.Zhou, and Z.Sun," A light weight and dependable trust model for clustered wireless sensor networks," in *Lecture Notes in Computer Science*, 2016, pp. 157–168, Springer, Berlin, Germany.
3. W. Luo, W. Ma, and Q. Gao, "A dynamic trust management system for wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 7, 2015, pp. 613–621.
4. J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*,vol.26, no. 5, 2015, pp. 1228–1237.
5. F. Ishmanov, S. Kim, and S. Nam, "A robust trust establishment scheme for wireless sensor networks," *Sensors*, vol. 15, no. 3, 2015, pp. 7040–7061.
6. T. Zhang, L. Yan, and Y. Yang, "Trust evaluation method for clustered wireless sensor networks based on cloud model," *Wireless Networks*, vol. 24, no. 3, 2016, pp. 777–797.
7. G. Rajesh kumar and K. R. Valluvan, "An energy aware trust-based intrusion detection system with adaptive acknowledgement for wireless sensor network," *Wireless Personal Communications*,vol.94, no.4, 2016, pp.1993–2007.
8. U. Ghugar, J. Pradhan, S. K. Bhoi, R. R. Sahoo, and S. K. Panda, "PL-IDS: physical layer trust-based intrusion detection system for wireless sensor networks," *International Journal of Information Technology*, vol.10, no.4, pp.489–494, 2018.

AUTHORS PROFILE

Maheswarareddy Anna Reddy studying as Research Scholar in Sunrise University Alwar, Rajasthan. He did his B.Tech ECE degree from Madanapalle Institute of Technology & Sciences 2004-2008.He did his Master of Technology from Jawaharlal Nehru Technological University Hyderabad (J.N.T.U.H) in 2010. He is a member of Professional IAENG (INDIA). My research interested in the areas of Wireless Networks, Embedded Systems, Digital Image Processing. Present working as Assistant Professor in the department of ECE in AITS College Kadapa, Andhra Pradesh. Published 8 papers in National and Internal journals and attended 5 National Workshops.

Prof. (Dr.) K.K. Saini Research Supervisor in Sunrise University. He did his BE (ELECTRONICS & COMM. ENGG.), ME (ELECTRONICS ENGG.) & PHD (ENGG.). He had also done MBA from Missouri University, USA by NFIS [Distance Education Centre] Harriman Circle, Bombay. He is expert & well known in the field of Electronics & Communication Engineering with a Experience of 25 years including Industry/Administration/Teaching.