Pattern Matching Algorithm for Providing Security and Recuding Power Consumption in Wireless Sensor Network

Vinoth Kumar.S[1] Anu Radha Devi.V.S[2] Chinnadurai.S.U[3] Janani.K[4]
[1]Assistant Professor [2,3,4]Student
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]SNS College of Technology Coimbatore

Abstract— *Wireless Sensor Network (WSN) is a network which consists of large number of tiny sensor devices and sensor nodes. These type of nodes have great sensing technology. Due to its wireless nature, they can be easily destroyed by attackers. So to provide security we will be applying some mechanisms. Mostly there are three main components that deal with security of Wireless sensor network, prevention, detection and mitigation. Protection of network is the most challenging issue for preventing the harmful types of attacks and for security issue in WSN along with information security application domains. In WSN there are two types of nodes and they are source node and sink node which are used for the transmission of the data. The main challenge against deploying strong security algorithms is that WSNs suffer from major constraints in terms of power and computing resources. We will be using pattern matching, which is one of the mechanism that can be used for security of WSN.*

Keywords— Wireless Sensor Network, Intrusion Detection System, Intrusion Prevention System, Pattern Matching, Security Goal

I. INTRODUCTION

The objective is to prevent and detect the attack from intrusion detection system (IDS) using pattern matching algorithm in wireless sensor network. Intrusion in WSN is a process of attack which is harm to the network resources and accesses the data which is highly confidential. WSN tend to compromise the security due to its wireless nature. The fast growing of technology, the network resource has to be secured by using advanced mechanisms. WSN can be deployed using Internet in most efficient way, In WSN any kind of attack can take place. Sensor nodes have great sensing and processing capability, security may not be provided with high accuracy. One of the drawback of sensor nodes is that, it doesn't have much computational power and replacement of batteries is not feasible.

Security algorithms for strong intrusion prevention are power/memory-hungry. Which leads to the Utilization of lightweight security algorithms which are less effective and suffer from security holes. Some of the prevention techniques such as cryptographic techniques, confidentiality, authentication and message integrity have been proposed to avoid security threats. The goal of IDS is to detect and prevent attacks based on observation of behaviour.

II. RELATED WORKS

This section, describes about the various categories and different types of IDS in WSN.

A. Security Types

For providing security in WSN we need the help of the below categories:

1) Key management: The process of establishing the cryptographic keys between the security nodes is the first technique for security and it will enables the data encryption and user authentication.
2) User Authentication and Data Encryption: The protocol which provides security are proposed for providing the security for the information which is stored in the database of nodes, which will not been hacked by the unauthorized persons. A request will be send to the base station for the purpose of secured data transmission.
3) Security of services: For the security purpose some specialized services is provided, like securing locality, secure data aggregation security and security of synchronizing time. They are the progress which is in recent research areas in WSN. Most of the protocols to provide security is based on specific assumptions regarding the type of attack occurred. In WSN, if an attack occurs and if intruder is weak, then the applied protocol can prevent him from damaging a sensor network. This can reach the security goal, by providing proper functionality. Suppose if the strong intruder tries to break into the network, a very high harmful attacking can be possible which is non-negligible.

B. Intrusion Detection Approaches

Here some of the merits and demerits of different types of IDS which are proposed in an on-going research activities as shown in figure 1.

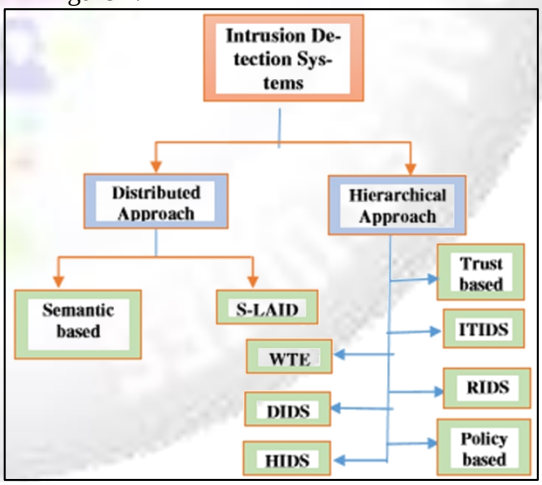

Fig. 1: Intrusion Detection Approaches

1) Distributed Approach

Based on semantics and multi agent IDS framework for WSN a technique is proposed. With the use of intrusion detection a very high security is provided by main functions of WSN based on formal semantics. Based on each selected semantic or rule, a mechanism is designed and that mechanism is mapped with the data that is sensed and collected by the sensor nodes for detecting an anomaly.

2) Hierarchical Approach

A model is mainly discussed based on trust, awareness and isolation detection mechanism including nodes compromised in WSN is proposed. It is mainly used for maintaining reputation and trust of sensor network. The hierarchical based IDS in a clustered network detect harmful or serious attacks. The main advantage of this model is, it can reduce energy consumption of sensor nodes. But with an increased rate of energy consumption with increase in cluster size.

III. INTRUSION DETECTION AND SYSTEM

The overview of the intrusion detection and its system for WSN and also analysis of pattern matching techniques is as follows.

A. Intrusion and Intrusion Detection

Intrusion is one of the activities that make the network to compromise with its security and especially the data confidentiality and its availability. To gain access to the network and acts as an authorized user, there are different types of attacks are possible. The main aim of IDS is to detect abnormal misbehaviour that cannot be halted by network's intrusion prevention techniques. Two types of abnormal misbehaviour are namely, malicious misbehaviour and selfish misbehaviour.

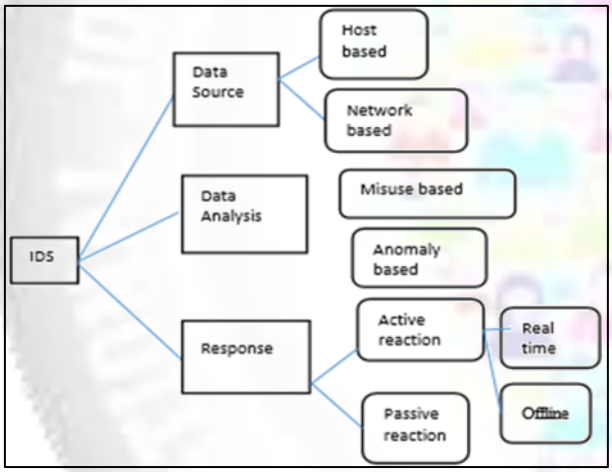

Fig. 2: Classes of IDS that can be designed in a system of WSN

The process of detecting such attacks caused by intruders and providing security to WSN is called as Intrusion Detection. It identifies unauthorized users and preventing them from accessing the network. The behaviour of the network is check by IDS and then it finds if the nodes are in normal operation. To ensure that the network resources can be protected, a simple unit can be installed either at client or server host. This unit is also known as IDS Agent. This agent acts as a gatekeeper which is used as normal node but detects the network using detection mechanisms. The IDS agents prevent malicious attacks and observe the behaviour of the network during flow of packet through communication channel. All the security protocols depends on the particular assumptions about the type of attack occurred. Once the attacker is "weak", the protocol will prevent an intruder from breaking into a sensor network and reaches the security goal, rendering its proper operation. If the attacker is "strong", a very high probability of an harmful attacking can be possible which is non-negligible. The intrusion detection, and also the mapping techniques are would help for mapping of data with the stored data. Three mapping techniques are: static mapping, dynamic mapping, control mapping. The classes of IDS that can be designed in a system of WSN, as described in fig 2.

IV. APPLICATION BASED TECHNIQUE

In methodology we deploy the IDS in WSN using pattern matching technique. The system is monitored for any type of security breach. Pattern matching detection techniques mainly uses set of signatures or rules for describing events that are undesirable. Whenever the pattern matches the data or any event, particular actions are performed. Then finally, IDS analyses the collected information of nodes in WSN and compares them with large set of signatures stored in databases of the nodes. The following steps are explained for the application using pattern matching technique.

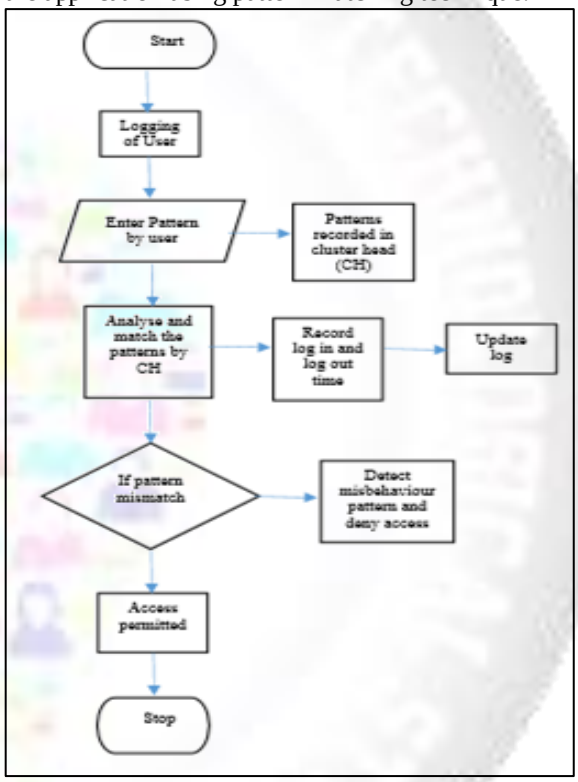

Fig. 3: Steps are explained for the application using pattern matching technique

- Step 1: User should login with the help of username and password for the purpose of specifying the user authentication.
- Step 2: Every user should create a specific pattern and it should be stored and recorded in the account of administrator. A centralized sensor node which is elected as a cluster head or an IDS agent is represented as an administrator. The patterns are consecutively stored each time the user logs in his/her account.
- Step 3: Those recorded patterns are analyzed every time and are matched with the previous patterns followed by the user pattern.
- Step 4: More than analyzing and comparing the patterns, the administrator will also keep track of time of login and logout of each user.

- Step 5: Even a small mismatch of patterns are to be considered, but if a high mismatch of patterns compared with current and previous patterns, then an alarm or alert will be generated and a warning will be provided to the user.
- Step 6: Once the user is given warning message, the user needs to reset the password by providing some of the security related data. The user can then recover the password.
- Step 7: In this way, the specific patterns are used in IDS for detecting malicious attacks.

The flowchart of the steps discussed above is detailed in fig 2.

V. INTRUSION DETECTION AND PREVENTION ALGORITHM

In this section, we discussed the algorithm used for pattern matching known as pattern matching algorithm for intrusion detection and prevention.

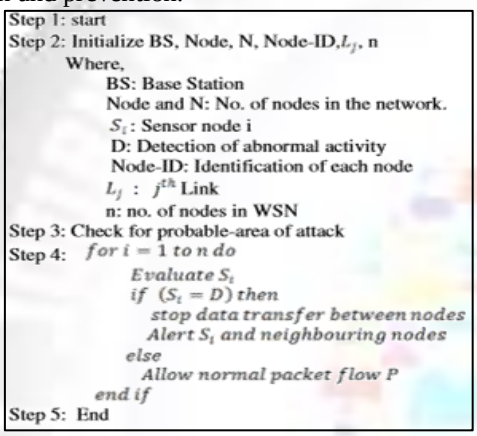

Fig. 4: Algorithm

In this algorithm, the cluster itself forms the sensor nodes sets after initializing the cluster heads. For each cluster, verification of authentication of each user is done by calculating the pattern bits and then goes through bit matching of patterns of each user.

VI. CONCLUSION

In our work we have tried to find the patterns used by the different users and match those patterns with the patterns that are stored in the database. We have applied a technique that, an alert will be generated as per the security concerns, if we find continues mismatch between the current and the previous patterns. The alert message will be send to the user. There by user get alert and protect their accounts. In this way this system will help the users to protect from the intruders.

REFERENCES

[1] "Pattern Matching Intrusion Detection Technique for Wireless Sensor Networks" Gauri Kalnoor1, Jayashree Agarkhed2 International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB16)

[2] "A Review of Intrusion Detection in 802.15.4-Based Wireless Sensor Networks" Mounib Khanafer; Youssef Gahi; Mouhcine Guennoun; Hussein T. Mouftah 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)

[3] "Distributed Trust based Intrusion Detection approach in wireless sensor network "Amol R. Dhakne; P. N. Chatur 2015 Communication, Control and Intelligent Systems (CCIS)

[4] "Preventing attacks and detecting intruder for secured Wireless Sensor Networks" Gauri Kalnoor; Jayashree Agarkhed 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)

[5] "Congestion control based on node and link in wireless sensor network"Xinhao Yang; Ze Li2016 35th Chinese Control Conference (CCC)

[6] "Data gathering mechanism of mobile data collector in wireless sensor network"Mrinal Kanti Deb Barma; Sudeshna Das 2016 International Conference on Internet of Things and Applications (IOTA)

[7] "Literature review of congestion avoidance system in wireless sensor network"Anuja A.Kadam;P.N.Chatur 2016 Second International Conference on Science Technology Engineering and Management

[8] Mohammad Saiful Islam Mamun, A.F.M. Sultanul Kabir, Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3 (July 2010)

[9] K.Q. Yan, S.C. Wang, C.W. Liu, A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks, Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 , Vol II 2009 ,Hong Kong (March 18 - 20, 2009)

[10] Yuxin Mao, A Semantic-based Intrusion Detection Framework for Wireless Sensor Network, Networked Computing (INC), 6th International Conference, Gyeongju, Korea (South) (2010)