ZigBee/IEEE802.15.4 표준을 사용하는 Ad Hoc 네트워크 상의 전력 통제

K.Kirubakaran*, 이재광*

*한남대학교 컴퓨터 공학과

Power control in Ad Hoc network using ZigBee/IEEE802.15.4 Standard

K.Kirubakaran*, Jae-Kwang Lee*

*Division of computer engineering, Hannam University.

Abstract

In this paper an intrusion detection system technique of wireless Ad Hoc network is explained and the advantage of making them work in IEEE 802.15.4/ZigBee wireless standard is also discussed. The methodology that is mentioned here is intrusion detection architecture based on a local intrusion database [1]. An ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. Due to increased connectivity (especially on the Internet), and the vast spectrum of financial possibilities that are opening up, more and more systems are subject to attack by intruders. An ideal IDS should able to detect an anomaly caused by the intruders quickly so that the misbehaving node/nodes can be identified and appropriate actions (e.g. punish or avoid misbehaving nodes) can be taken so that further damage to the network is minimized

I. Introduction[1]

An Ad-hoc network is a very particular network because it has no established infrastructure: it is a self-organized network where each mobile node is equipped with wireless interfaces. There is no centralized control (then, if a node fails, it won't cause the collapsing of all the network); then each node have to forward packets and so act as a router in order to allow the transit of information from a node to another. We also have to consider that mobile devices have power constraints (limited power, CPU, bandwidth and storage capacity), which can't enable them to do everything like the fixed devices.

In this paper we deal with the power constraint of the nodes and especially of the sensors that are used as IDS agents. By using ZigBee/IEEE802.15.4 standard [2] we diagnose the possibility of minimizing the power consumption of the sensors by making them communicate in beacon intermittent communicating mode. In this paper we have adopted an approach of applying the IEEE802.15.4 standard to an already existing IDS technique and enhancing that technique by reducing the power consumption of the active sensor nodes used as IDS agents.

In the remainder of this paper we start by briefly presenting the explanation of the

[1] This research was supported by the Program for the Training of Graduate Students in Regional Innovation which was conducted by the Ministry of Commerce, Industry and Energy of the Korean Government

existing systems in Section2. In section 3 we explain the characteristics and the advantage of the IEEE802.14.5/ZigBee standard. In section 4 we explain how the ZigBee standard can be inducted to the already existing IDS System. In section 5 we conclude by summarizing the strengths and the shortcomings of the new IDS technology.

II. Existing intrusion detection system

In their pioneering work on intrusion detection in Ad Hoc Andrew B. Smith the author of the paper[1] describes an IDS based on a Local Intrusion Database. In this paper[1] the mobile IDS agents are trying to extract the anomalies data so that it can trace out the intruder if there are any.

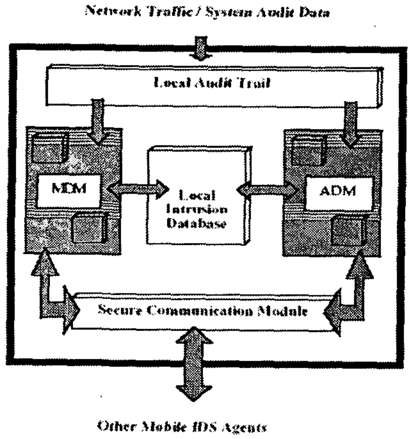

FIG 1. Mobile IDS Based on Local Intrusion Database

The FIG 1 describes the scenario of the IDS Proposed by A.B.Smith. The proposed IDS consist of 5 module and they are network traffic /System Audit Data, Local Audit Trail, ADM & MDM, Local Intrusion Database and Secure Communication Module.

Network Traffic/system auditData: The job of this module is to collect ad hoc network traffic data and system audit data.

Local intrusion database: This database is used to store all the anomalies. The data's stored here helps in tracing the intruder. The user can obtain information about the latest misuse signature and also find the latest patterns of normal user activity from this database. The secure communication module will then use this information for data mining of new anomaly association rules.

Secure communication module: This module acts as a moderator between ADM & MDM and other IDS agents.

ADM (Anomaly Detection Module) & MDM (Misuse Detection Module): This Module is helpful in detecting Anomaly.

III. ZigBee / IEEE802.15.4 characteristic.

In This standard, consumption of power is higher only at the cluster head in comparison with other nodes.

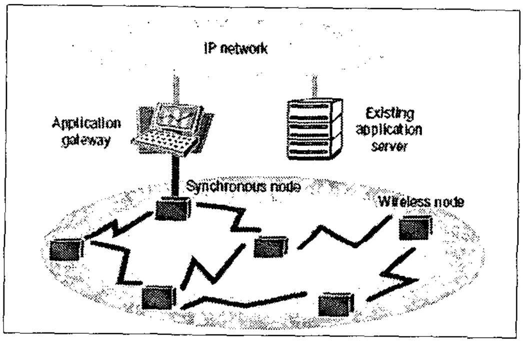

FIG 2. Feasibility testing scenario of the IEEE802.15.4.

The FIG 2 shows a testing scenario of the IEEE802.15.4. It shows the formation of the autonomous network between the wireless nodes, that can be either in CSMA-CA or TDMA. The TDMA makes static assignments of communication slots. Using a sleep function to conserve more power The CSMA-CA acquires communication slots while preventing collisions.

3.1 ZigBee / IEEE802.15.4 Advantage

ZigBee is the only standard that specifically addresses the typical requirements for wireless control and monitoring applications, such as: Large number of nodes. Very low system/node costs, Operation for years on in expensive batteries, Reliable and secure links between network nodes, Easy deployment and configuration

IV. Inducting the IEEE802.15.4 standard into the IDS

What if the IDS sensing agents present in every node are allowed to communicate within themselves using ZigBee/IEEE802.15.4 standard using a mesh topology? This will make the ids sensing agents to consume less power and to communicate between themselves in a form of clustered intermittent network so that the IDS agents are not required to be dependable on the secure communication module unless there are new anomalies (threats) that are detected and stored in the Local Intrusion database. The reason to form this intermittent communication network is to communicate the threats which an IDS agent comes to know in forehand with the other IDS agents.

This standard IEEE802.15.4 is involved only in the lower layers (physical and MAC layer). The major services performed here are establishment and termination of a connection, synchronization of the flow control (synchronization) and the modulation.

4.1. IDS components and the cluster formation

This section explains how the IDS agents from a cluster in order to communicate the threats. The cluster and the cluster head can be formed based on the hop counts [2].

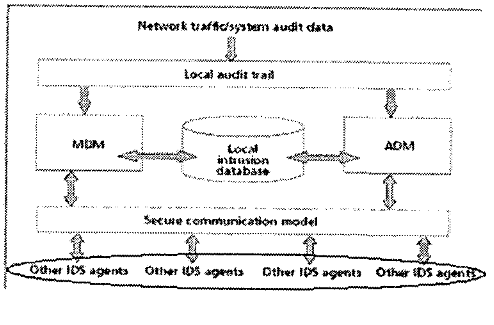

FIG 3. A Graphical representation of a Mobile IDS agent.

As, shown in the FIG 3 each individual IDS agents are combined to form beacon mode intermittent communication network.

The IDS agent which communicate with the Local intrusion database through secure communication model form a network and operates in various low power operating modes to save the power resource of the sensors.

The IDS agents can form a clustered intermittent network in a beacon mode among themselves by selecting one of them as the cluster head and communicating the threat details between each other. This is done to consume energy of the low powered sensor agent. In this way the communication between the agents are made more reliable with low delay time. As, this is a beacon mode of IEEE802.15.4 standard communication is triggered only when a sensor agent is facilitated (provided) with a beacon.

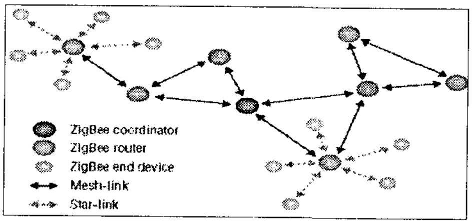

Fig 4. Network Model of ZigBee

The cluster and the cluster head can be formed based on the hop counts and the voting option of the nodes based on the highest connectivity index as in [3].But that is beyond the scope of this paper as we are concerned only with the power consumption of the IDS agents and the way to reduce it. Having said this it doesn't mean that we should not explain how cluster heads performs in the IEEE802.15.4 standard.

The cluster heads that are selected are designated as Coordinator and other IDS agent's acts as router and end devices. This is not a permanent setup as the IEEE802.15.4 is an autonomous technology it can alter the setting as when required.

So, the designation of the IDS agents

varies depending on which node precedes in gaining access about the anomalies / threats. As, shown in the FIg 5 and FIg 6. The cluster heads with the preceding knowledge of the threats acts as the coordinator. They can be interchanged with the other IDS agents that are acting as routers and end devices depending on the current threat knowledge.

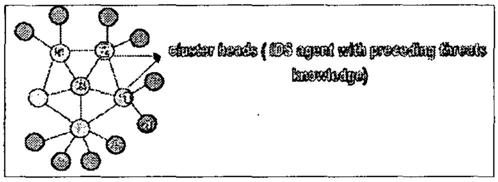

FIG 5. Autonomous network Cluster before cluster heads are inter changed

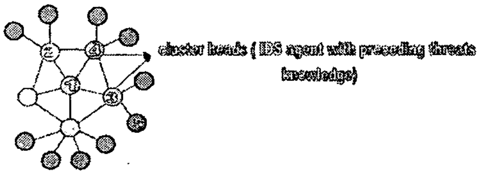

FIG 6.Autonomous network Cluster after cluster heads are inter changed

4.2 The principle behind the formation of the beacon mode network

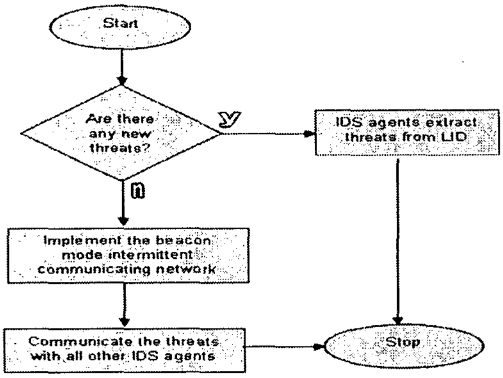
Start
Are there any new threats?
Y
IDS agents extract threats from LID
N
Implement the beacon mode intermittent communicating network
Communicate the threats with all other IDS agents
Stop

Fig 7. Flow chart describing the principles behind the formation of the beacon mode network

The flowchart in FIG 7 describes operation of the IDS agents to form an intermittent network. Initially the IDS agents search the Local intrusion database for new anomalies if there are any then they are extracted and used for the future purpose.

If there are no new threats and any of the IDS agent in a cluster doesn't have the knowledge of the existing anomaly then they communicate to them about that anomaly in a beacon mode intermittent communicating network.

V.Conclusion

This article presents a very new concept of utilizing the IEEE802.15.4 standard in the intrusion detection system. The cluster based beacon mode intermittent communication mentioned above has the distinct advantage of ZigBee/IEEE802.15.4 standard like uninterrupted communication with guaranteed bandwidth, low delays and low power consumption, a mechanism that prevents interference by other systems,

[References]

[1] AB.Smith, "An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks," 5th Nat'l. Colloq. for Info. Sys. Sec. Education, May 2001.

[2] Development of Ubiquitous Sensor Network, Shigeru Fukunaga et all, Oki Technical Review, October 2004/Issue 200 Vol.71 No.4

[3] Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks., Oleg Kachirski et all, (HICSS'03) 0-7695-1874-5/03 $17.00 © 2002 IEEE

[4] Intrusion detection in wireless ad hoc network, Amitabh mishraetal, IEEE Wireless Communications • February 2004

[5] www.mouser.com/chipcon

[6] Ad hoc networking, Perkins, Charles E. Addison-Wesley.

[7] Ad Hoc Wireless networks : architectures and protcols, Murthy,C.Siva Ram, Prentice Hall.