Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Immune System Based Architecture to Enhance the Security in WSN

Nipin Gupta
Research Scholar,
Jagannath University, Jaipur, India

Malay Ranjan Tripathy
Professor, ECE Deptt,
Amity University, Noida, India

Abstract: A Sensor Network is one of the most complex networks because of its low power sensing devices. In this present work we are building immunity system based architecture to secure the WSN. In this architecture the security load will be distributed in different intelligent sensor organs over the network. This load is divided in three main stages called prevention, detection and the network reconstruction. The prevention mechanism will be performed by the memory cell nodes. Responsibility of detection process is on T cells and the antibodies will perform the node blocking and the network reconstruction over the network. The whole system will be maintained by the brain cell that will perform the activation of these three security services respective to required security level. The presented architecture is reliable and improves the communication throughput over the network.

Keywords: Immune System, Authentication, Detection, Prevension, Architecture

I INTRODUCTION

A Sensor network is one of the most crucial and complex network because of its heterogeneity in terms of network type, topology, nodes and the application. A sensor network is constructed by the help of wireless tiny sensors with the minimum requirement of transreciving and sensing capability. The major vector in such network is network type, it represents the sensors can be implemented in any kind of network including the mobile networks, vehicular area network, body area network etc. Each kind of network has its own capabilities and the requirements. It means to work of sensor network we need to first understand the network type where it will be implemented. The major concern of the sensor network is the topology. Some of sensor networks can be centralized such as in body area networks and some sensor networks are randomly distributed and we can shape them such as the vehicular area based system. The topological architecture is also based on the application and the network requirement. According to these requirements the node type is also decided. In the simplest sensor type they only perform the transmission and do not have storage element or the processor. There also exist the smart sensors with the capability of the memory and the processors. The sensors also exist that can perform the required decision making in terms of security analysis, congestion control etc. Because of these all reasons there is always the requirement of some such architecture that can be implemented on any kind of sensor network respective to the service distribution. The AIS (Artificial Immune System) gives such kind of architecture.

In this architecture system the complete network is divided in controller nodes. Figure 1 is showing the three levels of the architecture. The level 1 is represented by the brain nodes. This kind of node is having the maximum configuration in terms of memory and the processing requirement. It works as the main centralized node which is responsible for all the communication over the network. All the

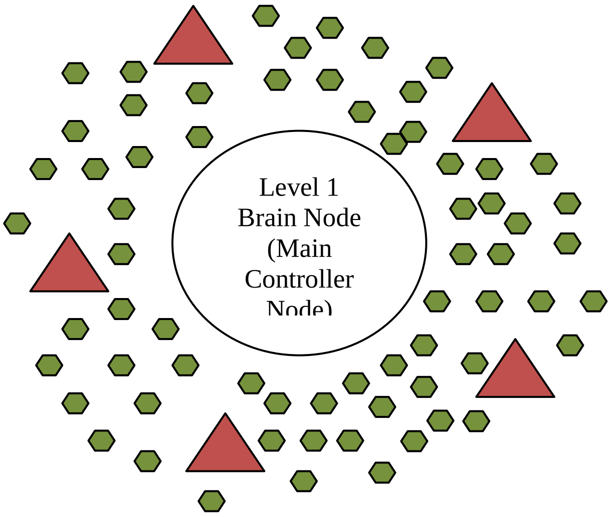

Figure 1: Artificial Immune System

Aggregative work or the decision making regarding the whole system is done by this brain node. It is responsible for the work distribution as well as the allotment of the services. It can also block the services or to prioritize them according to network or the application requirement. Any problem in such node can block or disturb the communication over the whole network. The second level of the categorization is in the form of agent nodes. As the sensor network system is a large system with different kind of services over the network. To control these sub systems over the network some agent nodes are defined with respective capabilities. In this figure 1 the rectangle shape nodes represents the agent or the controller nodes. These agent nodes are intelligent nodes that control the sub system with its defined strength and to report to the brain node. A network system has a few agent nodes depending on the physical distribution or the number of services that required to control over the network.

The third and the lowest level of node are the communicating sensor nodes. In figure 1 level 3 nodes are defined in green circles. These are vast number of nodes that can be homogeneous or the heterogeneous depending on the network type. These nodes have lowest level of physical characteristics in terms of energy, memory and processing capabilities. There also exist such nodes that do not have any memory or the processing capabilities.

II Security Architecture

As we discussed earlier the WSN is one of the most complex network as it can be implemented on other network types. Because of this the capabilities and the requirement such network change according the network type and the application. Because of this for the service capabilities and the network architectures is required to design respective to the system requirement where it will be implemented. To design the generic architecture there is lot of dynamic properties that is required to be discussed. In this work we are basically designing such a generic system that can be implemented on any kind of network system. The presented system is based on the immune system. The work is about to present this system respective to the security requirements of the system.

The security is always the major challenge for wireless or the dynamic network. There are number of factors that influence the security system. This factor includes the physical characteristics of the system, topology and the routing gateways. A network is affected from the internal and external attacks. The internal attacks are performed by some internal node or itself generated by some miscommunication within the network. The reason of these attacks is the high load over some node or the energy loss of a node. The kind of attack is done by the external nodes that are performing by some dynamic node that enter to the system with some fake identity. These attacks basically capture the network information or change the communicating data to add error in data values. To handle these all kind of attacks there are different kind of detection and the prevention mechanisms exist. These all are collectively called the security services.

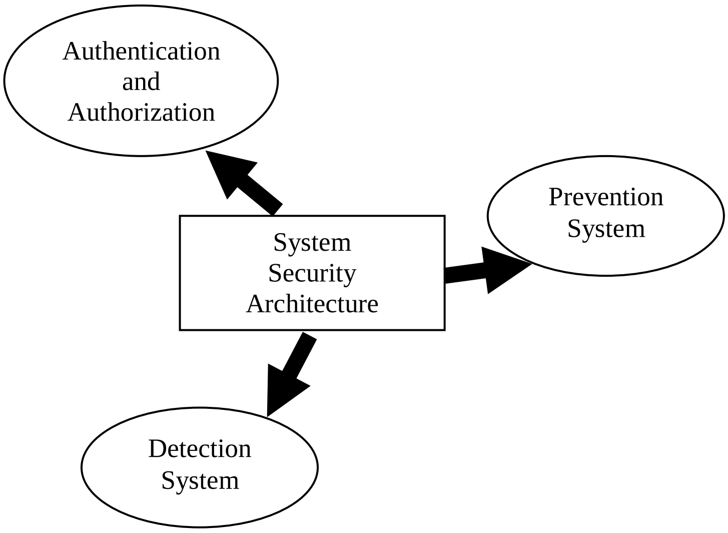
Authentication and Authorization
Prevention System
System Security Architecture
Detection System

Figure 2: Secure System Architecture

The authentication and authorization service is the major security approach used to distinguish the valid and the attacker node. Each node over the network is assigned a unique id. In first level of authentication system the communicating node is checked for the valid identity. The authentication is verified by the main controller node. In the second level the authorization is performed by the controller node. The authorization is basically used in heterogeneous systems where different communicating capabilities are defined for different kind of nodes. The work distribution respective to the secure communication is done at this level. In the third level of this service the secure communication is performed. For this communication the cryptographic algorithm is implemented. A key distribution and encoding approach is implemented to perform the secure and reliable communication over the network. Here figure 2 is showing the complete authentication and authorization system. As we can see the it is defined as a sequential security process in which the level of security is implemented in a series. With the implementation of all three sub systems the high level secure communication can be achieved. The system is basically to save the network from any kind of external attack. The system is safe in terms in case of different intruder attacks.

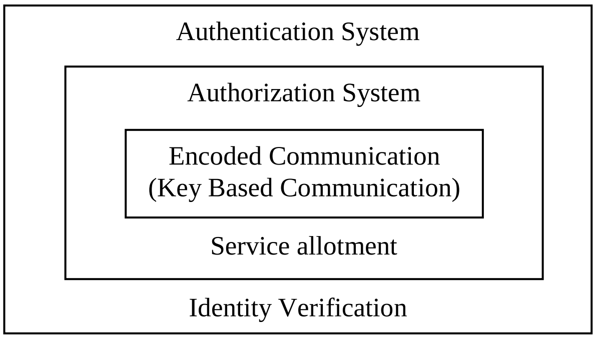

Figure 3: Authentication and Authorization System

The second major aspect of security architecture is prevention algorithm. The prevention approach is based on the existing network communication statistics. It includes the prediction oriented analysis to identify the chances of some attack or the data loss during the communication. Based on this analysis the early decision is taken place regarding the node blockage or the route change. The major concern in this kind of security service is the preventive path generation. According to this approach a compromising path is detected to perform the expected reliable communication. Let we have a network with m nodes called N=N1, N2, N3….Nm. From the initial analysis the list of attacker node list is generated called A=A1, A2….An. In case of preventive analysis the the communication path will be generated on nodes excluding the expected attacker nodes i.e.

$$SafeNodes=N-A$$

It means the safe path will node include any node that is in the list of expected attacker. To identify this kind of different algorithmic approaches are used such as ACO, Genetic approach etc. Generally this kind of preventive analysis is performed by the intelligent node with high memory i.e. Centralized nodes. Such kind of preventive mechanism is basically implemented to save the network from internal attacks.

The third and the main key of secure network architecture is the Detection System. This kind of system is the innermost layer of secure system architecture. This layer is called the Detection System. In case, if some smart intruder enter to the system and start to disturb the network in different ways, it is required to analyze the network and to identify the type of attack and the attacker nodes over the network. The work of this layer is divided in three sequential phases shown in figure 4.

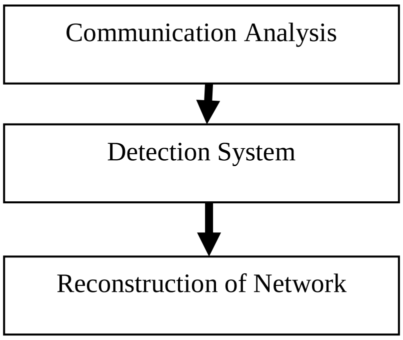

Figure 4 : Detection System

As we can see in the sequential definition of the detection system is shown. In the initial phase the communication analysis is performed. There are number of different approaches for such kind of analysis. These approaches can be centralized or the host based. In the centralized system the approach will be implemented on the main controller node that will perform the decision making on the basis of analysis on all nodes over the network. The analysis can also be performed on each host of the network. This kind of analysis is based on the neighbor node communication analysis. Another analysis type is the agent based analysis. In such kind of analysis we place some agent nodes over the network and these agents perform the analysis on neighboring nodes.

Once the analysis phase is done the detection system starts working. It is about to detect the attack over the network, for such kind of attack detection there are number of approaches. The detection systems are of two types, one is the attack specific detection system and other is the generic detection system. The generic systems are based on the throughput or the loss analysis based system. In both kind of system the most common approach among them is the threshold based analysis. According to this approach the threshold value is set to analyze the communication throughput on the each node on routing path. If the loss is greater than threshold value, it means there is some attack in the network. The threshold analysis can be performed on different communication parameters such as Network throughput analysis, loss analysis etc. The detection phase is performed on some specifc nodes and sometimes periodic to improve the network optimization.

The third and important phase of the detection system is the network reconstruction. The reconstruction includes node elimination, load distribution and the network rerouting. The reconstruction process is actually done by the centralized node or the agent. Once the reconstruction is done the network start behaving normally.

III Immune System Based Architecture

In the above defined security architecture we have defined the system in three security layers. These layers will be executed in a series from outer layer to the inner layers. This architecture is the parallel implementation of all three layers for complete network. But the sensor network has the drawback in the form of energy concern. Implementation of this complete system for the complete network is not efficient in terms of network delay and in terms of energy optimization.

In this work we have presented a security system that can be implemented on any kind of sensor network. The presented system is based on the human immune system. In this present work we have divided the complete network system in the form smaller sub system. Each sub system is having a controller agent to manage the security for that sub-system. These all systems are arranged in the form of human immune system. Different systems presented here work as different organs of the human body.

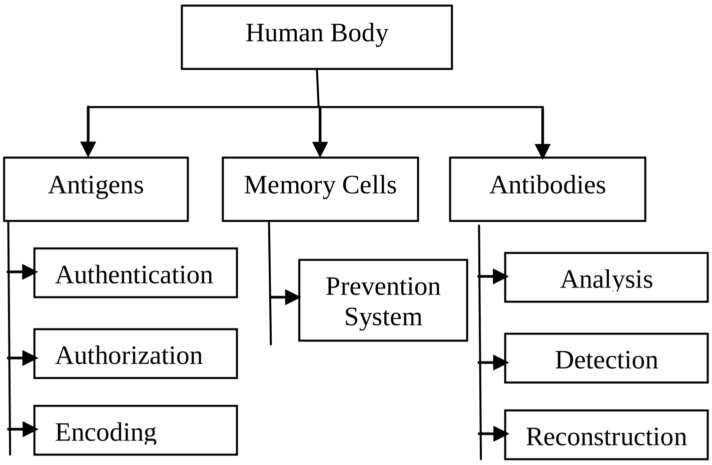

Figure 5 : Secure Immune System

As we can see the complete architecture proposed is shown in figure 5. We have divided the complete network body in three main sub systems called Antigens, Memory Cells and Antibodies. Each sub system is for some specialized task. These sub system further intake some other body components to perform sub tasks related to that system.

IV CONCLUSION

The proposed system is based on a immune system based architecture to improve the network security in wsn. We have divided the network in different clusters according to the work process. Each cluster is defined by some controller. Each controller is assigned by specific task of authentication or security. The presented system will give an enhanced protocol with security.

REFERENCES

[1] Suman Deswal and Sukhbir Singh, "Implementation of Routing SecurityAspects in AODV", InternationalJournal of Computer Theory and Engineering, Vol. 2, No. 1 February,2010.

[2] Chin-Yang Tseng, "A Specification-based Intrusion Detection System for AODV".

[3] Monis Akhlaq, "Addressing Security Concerns of Data Exchange in AODV Protocol", World Academy of Science, Engineering and Technology 16 2006.

[4] Mariannne. A. Azer, "Wormhole Attacks Mitigation", 2011 Sixth International Conference on Availability, Reliability and Security

[5] Pallavi Sharma Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", 978-1-61284-486-2 IEEE.

[6] Yih-Chun Hu, "Wormhole Attacks in Wireless Networks", I EEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

[7] Majid Khabbazian," Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS 1536-1276/09@ 2009 IEEE.

[8] Sergio Felperin," A Theory of Wormhole Routing in Parallel Computers", 0-8186-2900-2/92@1992 IEEE

[9] Jong-Pyng Li," Priority Based Real-Time Communication for Large Scale Wormhole Networks", 0-8186-5602-6/904 1994 IEEE

[10] Farid Na¨ıt-Abdesselam," Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol", WCNC 20071525-3511/07©2007 IEEE

[11] Xia Wang," An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks", 31st Annual International Computer Software and Applications Conference(C0MPSAC 2007) 0-7695-2870-8107@2007 IEEE

[12] Viren Mahajan," ANALYSIS OF WORMHOLE INTRUSION ATTACKS IN MANETS", 978-1-4244-2677-5/08©2008 IEEE

[13] Yun Wang," A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information", 2010 Fifth IEEE International Conference on Networking, Architecture, and Storage 978-0-7695-4134-1/10© 2010 IEEE

[14] Sanjay Keer," To Prevent Wormhole Attacks Using Wireless Protocol in MANET", Int'l Conf. on Computer & Communication Technology 978-1-4244-9034-/10©2010 IEEE

[15] E.A.Mary Anita," A Certificate-Based Scheme to Defend Against Worm Hole Attacks in Multicast Routing Protocols for MANETs", ICCCCT-10 978-1-4244-7770-8/10©201 0 IEEE