ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Optimization of Security Framework Mechanism Based on Local Knowledge Discovery Process for WSN

Sonika*, Rajeshwar Singh

* P.G Student, Department of ECE, Doaba Institute of Engg. & Technology, Mohali, Punjab, India
Professor, Department of ECE, Doaba Khalsa Trust Group of Institutions, SBS Nagar, Punjab, India

Abstract

Network security is a prime concern along with energy management in wireless sensor networks. Many application of wireless sensor network such as monitoring, tracking and priority processing of security are always dependent on available resources and available security measures. This research provides security framework with aggregation adaptive framework for network filtering process with add on feature of pattern matching process with frequent correlation with packet sequence. We have used free bit information in header for frequent correlated match of any malicious activity so that there is no need to go for the pattern matching with knowledge base of the network for the same type of events occurred in the network. Variation of security level has been considered with variation of attacker time. Our proposed framework provides 2 % less security level hitting values when tested with 300 collected periods and provides 5 % less security level hitting values when tested with 300 collected periods with variation of frequency of attack when compared to adaptive security framework. Proposed work provides less resource consumption and higher security level in aggregated view of context with stable authentication process.

Keywords: Adaptive Security, Collect Period (CP), Knowledge Discovery, Packet Delivery Ratio (PDR) Wireless Sensor Networks (WSN).

Introduction

Wireless Sensor Network (WSN) is an emerging field these days. Wireless Sensor Networks are very popular in the areas of environment monitoring, agriculture, military surveillance, healthcare and home security. Sensor Networks are not conventional computing contrivances [1]. The fundamental design of Sensor Network is to scatter tiny sensor devices which are capable of sensing some parameters and are also able to communicate with each other [2]. Sensor Networks possesses distinctive properties which are not there in traditional networks [3]. Architecture is the vertebrae of any network [4].WSNs consist of nodes for data gathering [5]. Fig. 1 shows the architectural view of WSN (Wireless Sensor Network). These sensing nodes collect the information from the deployed environment, process and compress it and then transmit it to the base station for further proceedings [5]. As Wireless Sensor Networks are keep on improving day by day and are being deployed in so many applications, the need of security is also increasing. No doubt there are number of mechanisms are available for providing security but no one from them is as much effectual that it can fulfill the need of security on WSNs. Wireless Sensor Networks, as already discussed in architecture section of this paper, are made up of small sensing nodes and these nodes are battery operated. These sensing nodes perform the task of sensing, computation and then processing of information. If we implement any security mechanism at nodes, then nodes must feel the shortage of energy which is required to keep them alive. And moreover the attacks from which the nodes suffer most may not be same every time. The attacker may interrupt the network in some different way. So, we need a security system which is able to adjust security level according to the attack. In this paper we are going to propose a security framework based on local knowledge discovery process which is able to adjust security according to the attack. The framework includes context module, security adaption module and security layer and for local knowledge discovery we are using two bits in our header. Whenever any malicious activity is found, its pattern is being matched with the existing knowledge base. And if some match is found then security scheme according to the severity of attack is being applied.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

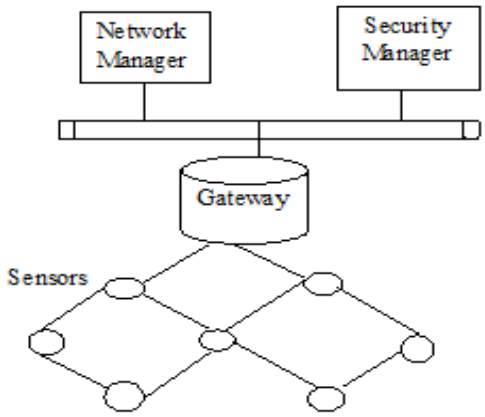

Figure- 1 : Architecture of wsn

The paper is structured as follows: Section II describes Related Work. Section III presents the architecture of the framework and simulation set up for proposed framework. Section IV focuses on the result and discussion. Section V presents the conclusion and future scope.

Related study

With the advancement in technology the wired networks are being on replacement with wireless. No doubt wireless networks are proving themselves very effectually in today's age but the constraints related to security specially are presenting a great challenge to the researchers. The related study shows that adaptive security is highly required in vigorous state of affairs. Security adaption means the designed framework is able to adjust security according to prerequisite. Basically Adaptive Security Provision is a routing protocol that comprise of optimized approach for escalating energy competence and security [10]. Ke Shi [8] proposed Adaptive Security System (ADAPSEC), a reconfigurable security architecture based on runtime dynamic reconfiguration. In ADAPSEC optimal security policies can be selected and imposed in sensor networks in accordance with the scrutinized external conditions, application requirement and internal resource constraints. In Adaptive Security System, the link & component layer are able to achieve vigorous configuration at run time. According to the prerequisite of application policies are designed which further decides the security.The two main components in ADAPSEC are: Policy definition & resolution module. 2) Policy enforcement. Kalpana Sharma et. al [7] have proposed Cross Layer Framework For Security (CLIFFs) in which they have proposed ASP (Adaptive Secure Communication Protocol). ASP is able to adjust itself according to security level required for the present state of the network. They have used ISA (Intelligent Security Agent) to determine the security level. Fang Lan et. al [6] proposed a scheme for network security situation awareness based on knowledge discovery process. The two main parts of their framework are Network Security Situation Modeling and Network Security Situation Generation. Their framework is useful for getting the real view of security level as it is based on security alerts. Laura Gheorghe et. al [9] proposed the Adaptive Security Framework (ASF) which is a modular and extensible framework which is able to adapt security based on detected threats, available energy, memory and security requirements. This framework includes: Security Adaption Module, the Security layer and the Context layer.

Architecture & simulation setup

Our research will focus on eliminating the wireless sensor network attacks. We will start with network analysis under NS2 Simulator. We will start with deployment of enterprise network structure based on wireless sensor network and unique keys will be assigned to the network nodes so that communication process will be secure.

The simulation randomly generates 50 points in the range of 1000m×1000m plane. The coordinate of the base station for whole network will be decided. Various energy values will be provided to nodes and base station. Magnify Coefficient value based on distance will also be assigned to simulation. Network filtering is used in term of event filtering, discovery of facts and instruction set based on network configuration. In related study, network security has been provided with security layer management with available memory process in which event for the particular security concerns in network has been fetched and then correlated with knowledge base of the already existing data. Sensors based on the filtering of network on different situations used to sense the type of situation and then compared with database available in the network, if any correlation found then process with suitable measure for prevention of this type of sequence.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

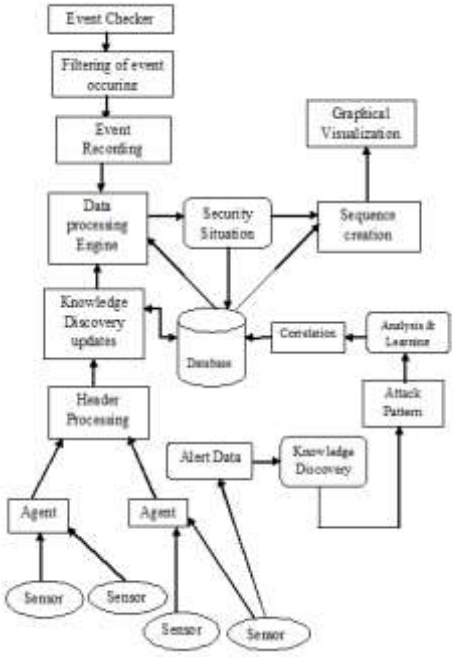

Figure- 2: Proposed Architecture

Pattern matching process is done with matching of security adaption on Specific time interval which has been used to provide exact information of the situation, which is further managed by context module. This scheme is good and providing good network filtering process but there is concern of resource consumption while matching on every interval of packet arrival. In our proposed scheme, which is shown in Fig. 2, we will be working on the similar architecture for network filtering process with add on feature of pattern matching process with frequent correlation with packet sequence. We will be carrying a 2 bit information in header for frequent correlated match of any malicious activity so that there will be no need to go for the pattern matching with knowledge base of the network for the same type of events occurred in the network. This information will be useful as it will not create any overhead to the header as we have 4 bit free information space in every header and we are using only 2 bit from it and can provide security efficiently with saving of time and resources.

Results & discussions

The proposed work use to simulate wireless sensor network implementation and proceeded with implementation of adaptive security based dynamic framework with minor changes of residual energy and programming of sensors in network simulator. At initial phase basic functionality and collection of information (simulator, basic mobility functions etc) has been done.

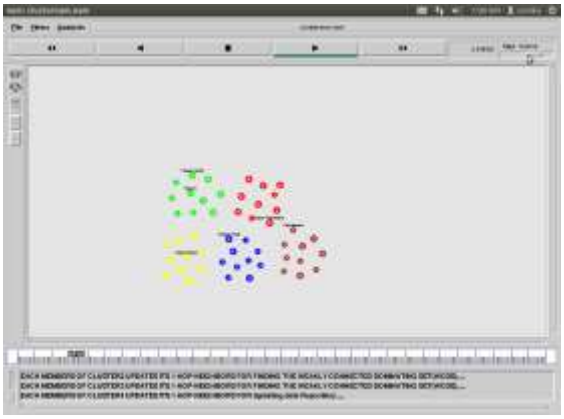

Figure- 3: Simulation Scenario For Experimentation

Network simulator has been used to provide the simulation and results of the proposed work. Grid area considered as logical based on network grid area nodes which represent the different area for the sensing ground. In Fig. 3, overview of the simulation has been shown. The transmitting and receiving power has been configured with basic energy carried by mobile nodes. The initial state is for selecting cluster heads based on the residual energy of the nodes. Further we have implemented a simple scenario for wireless sensor nodes and divided the grid area into equal parts. Mobility sensing process starts with computation and communication later on, as shown in figure 4. After this we have implemented the unwanted attack traces vary from single level to level 5 communications for showing the effects of attack on wireless sensor network. A proposed concept of adaptive security infrastructure attack detection is used to provide security preservation in wireless sensor network by hybrid history based counter bits to solve the issues created by database update and to provide local repository solution for saving of resources.

For experimentation we have used network simulator version 2 with animation for the concept of dynamically updating knowledge set for preventive solution of event generation by malicious traffic.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

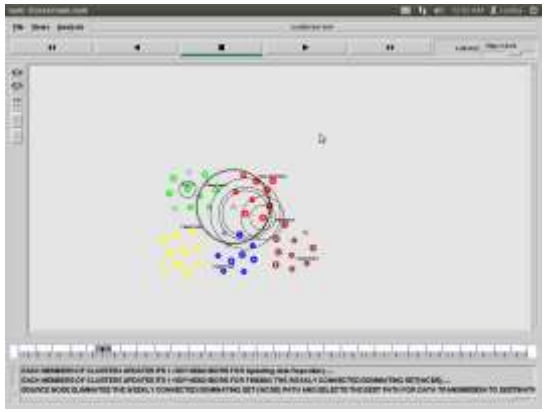

Figure- 4: communication scenario for proposed secure and hybrid history based scheme

In Fig. 4, concept of the communication implementation and detection of attack events is shown with updating knowledge server in network while communication of wireless sensor nodes to cluster heads and further cluster heads to base station.

A. Packet Delivery Ratio

Packet Delivery Ratio is defined as the ratio of number of packets received at the destination to the number of packets transmitted from the source.

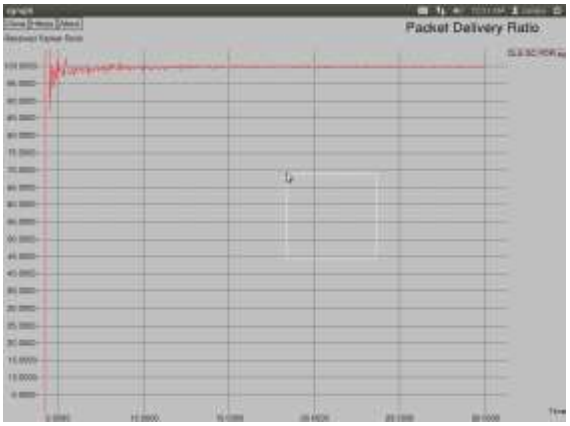

Figure- 5: Packet Delivery Ratio

Packet Delivery Ratio is always used to decide the performance of the network and its processes so we have considered the experimentation with packet delivery ratio with our proposed scheme. Fig. 5, shows the packet delivery ratio analysis for proposed work. Packet Delivery ratio is always decides the accuracy and cost of the network resources. Proposed work provides good solution of avoiding unwanted attack detection without spending much of resources in wireless sensor network.

B. Severity Level Hit Ratio with 10 CP (Collect Period)

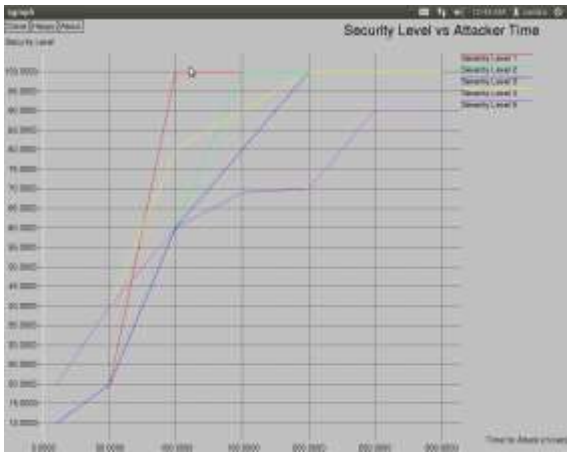

Figure- 6: Proposed scheme and existing scheme in term of security level when attack period is 10 times of CP

Security process is calculated by considering the collect period in term of attack period with collect period of 10 times. Comparison for the proposed work is done with existing security scheme based mechanism in wireless sensor network is shown. Fig. 6 shows the comparison shows that severity level hit of the proposed work is less. Higher and faster security level have been achieved and shown in proposed work is higher than shown in previous techniques due to secure communication with lighter algorithm model based on optimization of header values with secret key exchange mechanism. Our proposed framework provides 2 % less security level hitting values when tested with 300 collected periods with collect period is 10 times represented as attack period.

Further we have extend our experimentation to check the efficiency of the code by taking attack period 20 times of collect period.

C. Severity Level Hit Ratio with 20 CP (Collect Period)

Security process is calculated by considering the collect period in term of attack period with collect period of 20 times. Comparison for the proposed work is done with existing security scheme based mechanism in wireless sensor network is shown.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

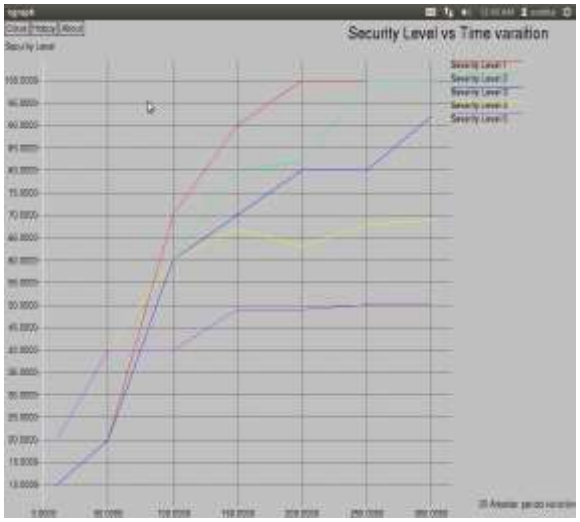

Figure 7: Proposed scheme and existing scheme in term of security level when attack period is 20 times of CP

Fig. 7 shows the comparison shows that severity level hit of the proposed work is less. Our proposed framework provides 5 % less security level hitting values when tested with 300 collected periods with collect period is 20 times represented as attack period.

Conclusion & future scope

Variation of security level has been considered with variation of attacker time. Our proposed framework provides 2 % less security level hitting values when tested with 300 collected periods and provides 5 % less security level hitting values when tested with 300 collected periods with variation of frequency of attack when compared to adaptive security framework. Proposed work provides less resource consumption and higher security level in aggregated view of context with stable authentication process by hitting severity level varies from level 1 to level 5 and attaining network hit period lower than the previous stats for severity hit in wireless sensor adaptive security framework. The proposed scheme provided successful mechanism for detection malicious attack traffic. In this present work, we have considered various traces and header processing for decreasing resource consumption in innovative way to attain security by maintaining local process for event checking. This research hasn't considered the local repository process which can filter out genuine traffic with little misbehavior as it is also filtered. It is very interesting to apply present work with presence of honey pots which are useful in efficient event filtering along with local repository processing.

References

1. Abror Abduvaliyev, AI-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman, Wai-Choong Wong (2013) "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communication Surveys & Tutorials, 2013.
2. AI-Sakib Khan Pathan, Hyung- Woo Lee, Choong Seon Hong (2006) "Security in Wireless Sensor Networks: Issues and Challenges, ICACT, Feb. 20-22, 2006, pp. 1043-1048.
3. Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI (2012) "Wireless Sensor Network: Security Challenges", IEEE, 2012, pp. 68-72.
4. Daniel E. Burgner, Luay A. Wahsheh (2011) "Security of Wireless Sensor Networks", Eighth International Conference on Information Technology: New Generations, 2011, pp. 315-320.
5. D.G Anand, Dr. H.G. Chandrakanth, Dr. M.N. Giriprasad (2012) "Security Threats & Issues in Wireless Sensor Networks", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1, Jan-Feb 2012, pp.911-916.
6. Fang Lan (2010) "A Framework for Network Security Situation Awareness Based on Knowledge Discovery", IEEE International Conference on Communications and Network Solution, August 2010.
7. Kalpana Sharma, M.K. Ghose (2011) "Cross Layer Framework for Wireless Sensor Networks", International Journal of Security and its Applications, January 2011, Vol. 5, No. 1, pp. 39-52.
8. Ke Shi, Xuan Qin, Qifei Cheng, Yidong Cheng (2009*)* "Designing a Reconfigurable Security Architecture for Wireless Sensor Networks" IEEE World Congress on Software Engineering, 2009,pp. 154-158.
9. Laura Gheorghe, Razvan Rughinis, Nicolae Tapus (2012) ''Adaptive Security Framework for Wireless Sensor Networks'', Fourth IEEE International Conference on Intelligent Networking and Collaborative Systems, 2012, pp. 636-641.
10. Mohamed Younis, N. Krajewski, and Osama Farrag (2009) "Adaptive Security Provision for Increased Efficiency in Wireless Local Networks", Ninth IEEE International

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Workshop on Wireless Local Networks (WLN), 2009, pp. 999-1005.

Author Biblography

	**Sonika** P.G Student in ECE Deptt. at Doaba Institute of Engg. & Technology. She has done her B.tech (ECE) from Adesh Institute of Engg. & Technology, Faridkot, Punjab. She is also working as Astt. Prof. in the deptt. Of ECE at DKTGI, Rahon, SBS Nagar, Punjab.
	**Rajeshwar Singh** presently working as Director, DKTGI, SBS Nagar, Punjab. He received his Ph.D. Engineering degree from Deptt. of ECE, Faculty of Engineering, BIT Sindri, Dhanbad, Jharkhand. His Master of Engineering degree is in ECE with specialization in Digital Systems from Motilal Nehru Regional Engg. College (currently NIT), Allahabad, U.P. He received his AMIE (India) degree from The Institutions of Engineers, Calcutta. He has also received MBA degree in Information Technology from MD University, Rohtak, Haryana. He has more than 22 years of experience in teaching and industry. He has published more than 50 papers in national and international journal/conferences of repute.