ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY OF NETWORK CONTROL INTRUSION DETECTION SYSTEMS

Mr. Pradeep A. Patil*, Prof. Durugkar S.R
[*] S. N. D. College of Engineering and RC Yeola, Savitribai Phule Pune University
Assistant Professor Dept. of Computer Engineering Savitribai Phule Pune University

DOI: 10.5281/zenodo.229858

ABSTRACT

This proposed system is smart security framework for those applications where wireless and sensor network control systems are commonly used for in automation which reduces the time required to perform it manually and collective nature of wireless networks brings many advantages where it will be hard to achieve through wired approach to be used for monitoring and control; In this way, plays a vital role and ultimately will become the necessary requirement to have a highly reliable and industrial system which will immediately responds to events in real time fashion but with accurate actions.

To achieve the substantial security level in wireless sensor networks and intrusion detection system there will be only solution which is proposed in this system which will provide protection against attacks, energy-consumption and it would be preferred to activate protection only when needed. In given paper where we have stated that how packet-based selective encryption will be good for reduce energy consumption, and to detect when an attack can occurs;

To achieve the security in any domain is hard to achieve and because of this it is also hard to implement and maintain in wireless sensor network today is security. As WSN consists of nodes and sensors and the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a various potential attacks in networking; There is also an integral power and memory limitations of sensor nodes makes security solutions unfeasible and hard to implement which is not actually acceptable in WSN systems.

KEYWORDS: Wireless Sensor Networks, Digital Signature, Energy-efficiency, Networked Control System, security, wireless transmission.

INTRODUCTION

Providing a security in computer applications is became an important and necessary issue nowadays; but the monitoring of network to check whether attack is occurring or not will cost a lot and controlling those attacks will be a critical task and definitely complex to implement. Ultimately the interaction will go through packet-based networks among different subsystems is important but, the at the same time problems may occur while achieving the confidentiality and data integrity Security attacks could compromise the data and that is not acceptable in computing; such things are critical and important due to sensitive nature where networked control systems are used to operate in dangerous environment (Mechanical, chemical plant) or in critical scenarios. Such systems where we are getting shared distributed networks of sensors and mechanism which interacts with the physical objects and the system will be monitored and controlled by a supervisory module and data acquisition system.

Fig 1 Security in Computer Systems

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

In this proposed work, we consider misconception attacks which affect the data integrity of packets by establishing their payload. In particular, we assume that a central system of the network is interfered, so that it relays damage packets. The attacker can disturb either command packets 'u' or quantification packets 'y' or both. In general, Network Control Systems present many tests due to the time variable delays and packet dropouts.

This work does not focus on them and we assume stability for granted. Digital signature increases energy consumption mainly due to the increased size of the communicated packet. This could be a problem in case of battery powered wireless devices which are acquisition interest in factory automation Traditionally, energy optimization focuses on the digital part of the system and on the executed software; well-known energy-saving techniques can be either hardware (HW)-based [1] or SW-based In the context of networked embedded systems, it is conventionally known that communications play a important role in energy consumption and, for this reason, energy well-organized show strategies have been intended recently While energy overhead can be tolerated during an attack, it signifies a waste of resources when the attack is not active. Therefore, the most important issue to enhance system resources is intrusion detection. We study methods to detect an attack and to alleviate its effect on the NCS from the point of view of both performance and impairment. Clearly, there is a deal between security and performance and the proposed approach can be combined with such literature to find an optimal configuration. Usual techniques to protect packets' integrity are based on digital signature, which appends an encrypted summary of the message to the message itself. If the attacker perverts such a message, its presence is revealed.

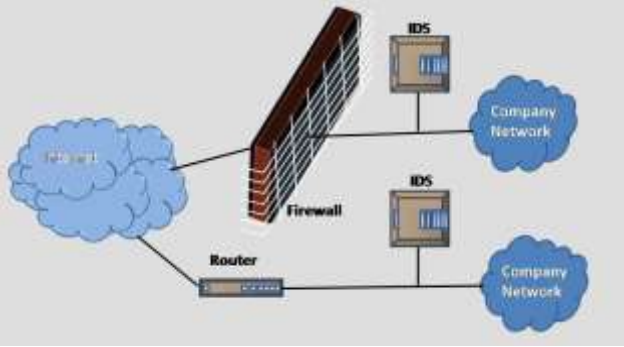

Fig 2 IDS Environment

In the context of control systems, some attacks have been intended to be virtually untraceable Past literature shows that intrusion detection is an open problem Furthermore, in a simple example at the beginning of the paper, we will show that packet deception cannot be detected simply by looking at the control concert since in many cases, injected data are not distinguishable. Customary anomaly-based intrusion detection systems perceive traffic of network and make comparison between established baselines. The standard will recognize what is "normal" for that network, what type of bandwidth is commonly used, what protocols are used, and what ports and devices generally connect to each other. Even if applied to control applications traditional approaches are for "formal" or "network-oriented" anomalies and it analyze the content of packets from the point of view of a control application. For example, altered commands elated by a formally precise protocol are not detected by traditional IDS.

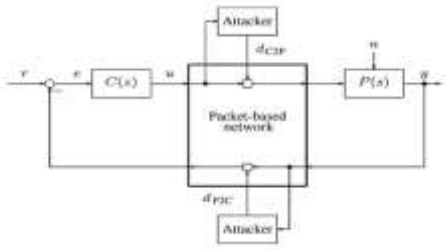

Fig.3 Block diagram of an Network control system

In particular, we propose the selective encryption of the packets exchanged between controller and plant which is required in the industry automation where we wish to implement the IDS to avoid harder consequences. From one side, this technique should eliminate damage risks and performance loss; however, from the other side, it should preserve the possibility to detect that the attack is over, so that resource consumption can be reduced. And we

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

present an attack-detection methodology based on the comparison between encrypted and unencrypted commands. Selective encryption was used to guarantee different levels of smart meter privacy and to reduce energy consumption in wireless communications, e.g., for the transmission of voice and ECG data. Another issue is attack mitigation, i.e., the countermeasure to be adopted when an attack is detected.

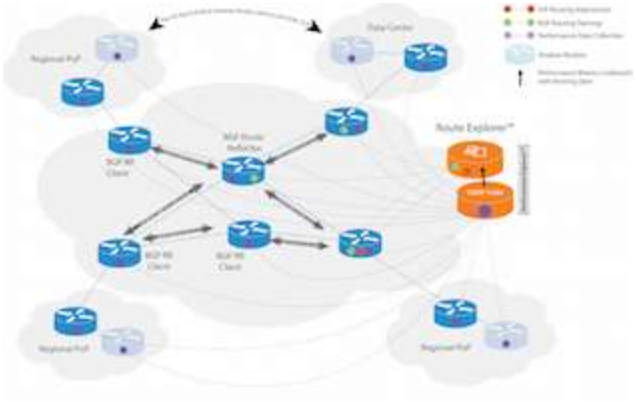

Fig 4 Packet Based Network

Attack mitigation has been addressed in the context of wireless transmission where the wireless nodes are present and most of the attacks succeed in the same where data will be compromised. Smart grid applications In this work, we propose to encrypt all the packets of the flow under attack except some anchor packets to detect when attack is over. Innovative work on the impact of packet losses on control performance shows that not all packets are equally important, this suggests to further improve energy efficient by varying the packet transmission rate according to the control performance .All these mechanisms need an extended architecture, which is also presented in this paper. The components of this architecture are suitable to be embedded in smart devices by following the guidelines study in the literature of survey. This proposed system is organized as follows where proposed architecture is describe for energy-efficient intrusion detection and mitigation of attacks and reducing the energy of nodes will be achieved.

RELATED WORK

Solutions to security attacks against wireless sensor networks involve many components such as prevention, detection and mitigation. First, we discuss the intrusion detection components.

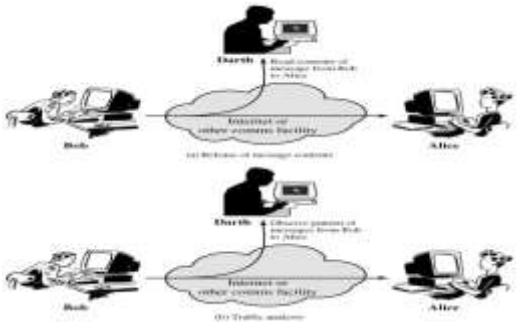

Fig 5 Attacks in Computing

According to detection means being aware of the attack that is present. So if an attacker manages to pass the measures taken by the "prevention" step, then it means that there is a failure to defend against the attack. At this time, the security solution would immediately switch into the „detection „phase of the attack in progress and specifically identify the nodes that are being compromised In WSN, sensor nodes use batteries as power supply so battery power is a significant resource for sensor devices. . ID systems are used to monitor both user and system activities to analysis any abnormal activity patterns and recognize patterns of typical attacks. The sensor nodes can be installed in an extensive geographical space to observe physical phenomenon with adequate precision and dependability. After installed, the minor sensor nodes are usually unapproachable to the operator. Therefore, conservation of energy and energy efficient routing must be taken into account when choosing a clustering algorithm.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Gaurav Jolly, Mustafa C. Kuşau, Pallavi Kokate, and Mohamed Younis
This Paper proposed key management feature of the security functionality.

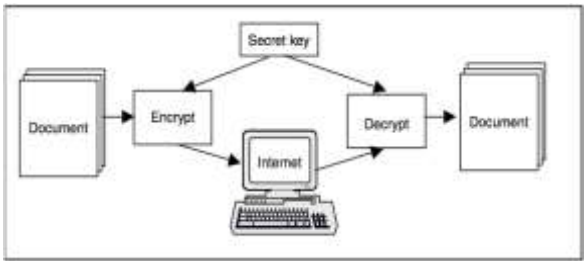

Fig 6 Encryption and Decryption

Secure key management is Important for any cryptographic security system. Energy-aware strategy for managing the cryptographic keys in a clustered sensor network. Shared symmetric keys are positioned into the sensors and gateways,

Hari Balakrishnan, Wendi Rabiner Heinzelman and Anantha Chandrakasan.
In This paper proposed the LEACH (Low-Energy Adaptive Clustering Hierarchy), the name itself suggest that it is adaptive in nature and it is a clustering-based protocol which utilizes non sequential rotation of local cluster base stations CHs to evenly spread the energy load among the sensors in the network LEACH uses regional coordination to enable scalability so that maximum nodes can be accommodated and strength for dynamic networks, and compound data will be integrated and will be sent with the routing protocol and idea is to reduce the amount of data that must be transmitted to the base station.

Manal Abdullah, Ebtesam Alsanee, Nada Alseheymi
This paper proposed an Intrusion Detection system which is mainly based on Stable Election Protocol only for clustered heterogeneous Wireless Sensor Networks.

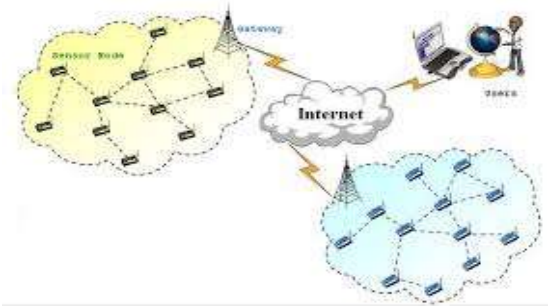

Fig 7 Wireless Sensor Network

The advantages of using SEP are that, it is a to prolong the time interval before the death of the first node.

Paria Jokar, Hasen Nicanfar, Victor C.M. Leung
In our IDS the normal behavior of the network is defined through selected specifications. But in this papers they have further investigated the physical and MAC layer attacks in Zigbee networks and also evaluate the performance of IDS . They Proposed IDS witch is a good election capability against known attacks, and since this IDS based on anomalous event detection,Chris Clark1, Wenke Lee2, David Schimmel1, Didier Contis1, Mohamed Kone2, Ashley Thomas2

This paper discusses the computation and interaction characteristics of typical intrusion detection. This paper describes efforts in mapping these tasks to a hardware platform using COTS components, this paper report the performance of proposed prototype NNIDS implementation and provide analysis on how the network processor architecture is definitely affect the performance.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Ozgur Depren, Murat Topallar, Emin Anarim, M. Kemal Ciliz
The proposed anomaly detection module uses a Self-Organizing Map structure to model behavior. Divergence from the normal behavior is classified as an attack. The targeted misuse detection module uses J.48 decision tree algorithm to differentiate various types of attacks. The main interest of this work is to make benchmark the performance of the targeted hybrid IDS architecture by using KDD Cup 99 Data Set.

CHALLENGES IN SYSTEM

In various applications IDS are used to monitor and control the Network; in which receiver will detects the attack as soon as data's confidentiality is compromised. The basic assumption is that it should be calculation infeasible to make a valid signature for a party without knowing party's private key.

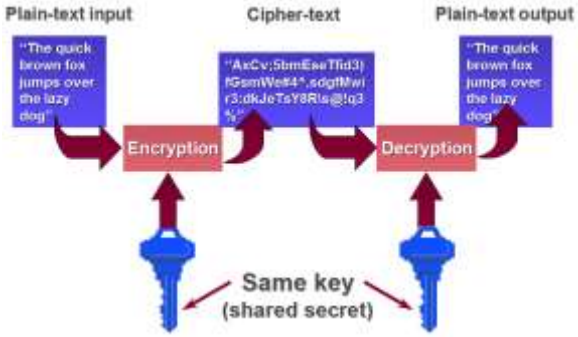

Fig 8 Symmetric key encryption

We are observing the symmetric key scenario used in above figure; To detect also replay attacks, a counter can be inserted in the signed message.

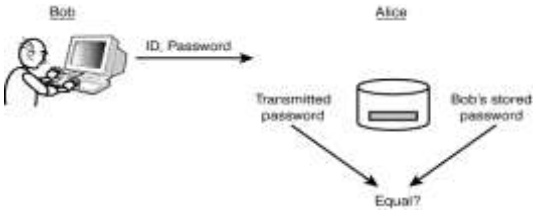

Fig 9 Message over Transit

In this work, we assume the presence of an end-to-end security protocol where ultimately we wish to maintain data secure. In other words, packet signing and integrity check can be performed at controller and plant side while intermediate network devices having task of relay packets up to the destination. In this way, various attacks on a tampered network device cannot modify signed data without being discovered which will be our final objective behind using IDS. If the attacker knows the transmission protocol, it is assumed that whether a packet contains a message signature and then only there will be chance to say data's security will be compromised. Therefore, without loss of generality, in this work, we just define a signed message as "encrypted" and we assume that the attacker should not alter it to stay hidden i.e. a kind of man-in-middle attack where an attacker will sit in between the sender and receiver.

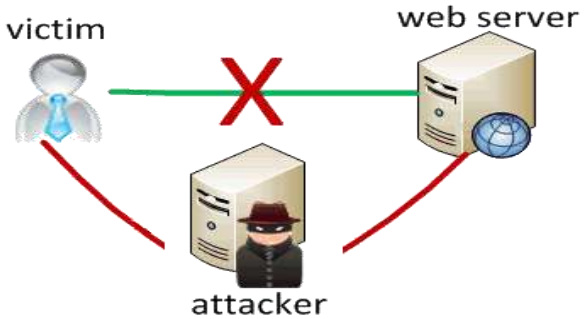

Fig 10 Man in Middle Attack

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Wireless networks are particularly prone to security attacks since the attacker does not need to tamper the wire to listen communications. In this work, we are interested in message corruption, as it can lead to severe damage of the NCS. Therefore, we assume a "man-in-the-middle" attack approach, which changes the messages in a tampered intermediate node according to the attacker strategy. Attack countermeasures are based on several encryption methods, classified into symmetric, e.g., Advanced Encryption Standard (AES), and asymmetric (e.g., RSA). To assess message integrity, digital signature is used. In this scheme, the message signature is generated by the sender by encrypting a short digest of the message using sender's private key; digest is created using a hash function known also at receiver side; the signature is transmitted together with the message; the receiver decrypts the signature with sender's public key and compares the result with a locally computed digest; if they are equal, the message integrity is verified. While performing the above mentioned activity they is lots of Energy get consumed during the exchange of key ,exchange of date and in checking the Intrusion in packets for that energy efficient system is needed witch is we are have proposed in this system.

In Industrial WSNs, designing scalable network architecture should be a primary importance. One of the designs approaches is to deploy homogeneous sensors and program each sensor to perform all possible application tasks.

Fig 11 Handling WSN nodes

Such an approach yields a flat single-tier network of homogeneous sensor nodes. An alternative multitier approach is to utilize heterogeneous elements. In this approach, resource-constrained low-power elements are in charge of performing simpler tasks which must be considered in WSN applications, such as detecting scalar physical measurements, while resource-rich high-power devices perform more complex tasks which varies with the nature of applications.

PROPOSED SYSTENM

The intrusion detection mechanism is implemented in the Security Check blocks while the adaptation of transmission rate according to the instantaneous control performance is performed in the Performance Check block; that will be described in detail in the specific sections;

Here, we list the meaning of the other blocks. Controller C(z): It is a discrete-time system running atFc, with Fc ≤ Fs, where Fs is the maximum sampling frequency the feedback system can run. It computes the command u to be sent through the network based on the tracking error e = r − y, where r is the reference and y is the decrypted measurement received from the plant (or its down-sampled version y DS). The difference equation describing C(z) is parametrized on the sample time Tc = 1/Fc to allow the controller to be easily adapted to a different sampling frequency.

Encryption block: This system encrypts a fraction of the incoming packets. E = 1 means that the current packet is encrypted and E = 0 means that the packet content is unencrypted. Encryption means that the signature of the message is inserted in the packet.

Decryption block: This block checks whether the packet is encrypted and, in this case, it verifies the integrity of the contained message; if an alteration is found, the attacker is revealed. It is worth noting that the proposed intrusion detection mechanism is not performed by this block; in fact, we assume that the attacker is smart and it does not corrupt encrypted packets to avoid to be revealed.

Plant P(s): A continuous-time system with input u (orits down-sampled version u DS) and output y.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Selector: The behavior of this block depends on the output of the Security Check block; if an intrusion is detected (A = 1 in the controller-to-plant channel or B = 1 in the plant-to-controller channel), the selector discards unencrypted packets, so that they are not used since their content is not trusted.

Attacker: The attacker tampers only unencrypted packets. In this work, we assume additive corruptions of the commands sent by the controller to the plant.

CONCLUSION

We proposed a system which emphasizes on energy-efficient security-aware wireless control architecture which resolves power issues in WSN and also detects the various attacks. We have assumed that the intrusion is hard to be distinguished from normal disturbance which must be identified and controlled. Encryption-based packet protection is energy-consuming for battery-powered devices which may consider as one of the challenge in WSN. We also showed how the number of encrypted packets can be adapted according to the presence of the attack, so that more energy is used only when needed. Since packet transmission consumes energy, we also proposed to adapt transmission rate to instantaneous control performance. Simulation results showed that the technique promptly reacts to attacks while energy saving was demonstrated analytically.

ACKNOWLEDGMENT

I would like to take this opportunity to express my heartiest thanks to my project guide Prof. Durugkar S.R. for his esteemed guidance and encouragement, especially through difficult times. His suggestions broaden my vision and guided me to succeed in this work and learnt many things under his leadership.

REFERENCES

[1] Adrian Perrig, John Stankovic, David Wagner, “Security in Wireless Sensor Networks” Communications of the ACM, Page53-57, year 2004
[2] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, International conference on Advanced Computing Technologies, Page1043-1045, year 2006
[3] Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, AdHoc Networks (elsevier), Page: 299-302, year 2003
[4] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, “A Survey on Sensor Networks”, IEEE Communication Magazine, year 2002
[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006
[6] Gerhard P. Hancke ,Vehbi C. Gungor, “Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches, , Senior Member, IEEE
[7] Dr. G. Padmavathi, Mrs. D. Shanmugapriya , “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”
[8] Riccardo Muradore, Davide Quaglia, Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 11, NO. 3, JUNE 2015
[9] Manal Abdullah, Ebtesam Alsanee, Nada Alseheymi “Energy Efficient Cluster-Based Intrusion Detection System for Wireless Sensor”, International Journal of Advanced Computer Science and Applications,Vol. 5, No. 9, 2014.
[10] Ozgur Depren, Murat Topallar, Emin Anarim, M. Kemal Ciliz* An intelligent intrusion detection system (IDS) for anomalyand misusedetection in computer networks Expert Systems with Applications elsevier 29 (2005) 713–722
[11] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan“Energy- fficient Communication Protocol for Wireless Microsensor Networks” Proceedings of the 33rd Hawaii International Conference on System Sciences – 2010
[12] Gaurav Jolly, Mustafa C. KuşÁu, Pallavi Kokate, and Mohamed Younis “ A Low-Energy Key Management Protocol for Wireless Sensor Networks”