ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 4, April 2016

Wireless Sensor Network security by Intrusion Detection in Energy Efficient Way

P N PRAJITHA
P G SCHOLAR
PPG INSTITUTE OF TECHNOLOGY

T POONGODI
ASSISTANT PROFESSOR
PPG INSTITUTE OF TECHNOLOGY

Abstract: Energy efficient algorithms for wireless sensor networks are getting popularity in the recent past. This paper describes a scheme for intrusion detection framework for clustered sensor networks. The primary design goal of a battery equipped wireless sensor nodes is to optimize the transmission energy. The proposed idea has the advantage that the communication and computation overheads are low and give better performance in terms of energy efficiency and intrusion detection. The paper proposes an energy-efficient architecture that is security aware for wireless control systems that may be used in factory automation. The intrusion and normal disturbance are very similar that it is hard to distinguish. The design become more complex since any protection leads to energy consumption and the design should take care to mitigate this by activating protection only on intrusion incident. Selective encryption for packet-based communication is worked out in this paper to reduce energy consumption, and to detect when an attack occurs in the system. Packet transmission rate is also a factor for energy consumption, the design also adapt according to instantaneous control performance.

Index Terms—Intrusion, detection, network, sensor, authentication

I. INTRODUCTION

Wireless sensor network (WSN) is gaining high criticality due to rapid development and deployment in hostile environment, and is vulnerable to a wide range of attacks. A WSN is a large network of resource-constrained sensor nodes with multiple preset functions that transmit environment related data to sink node. WSN consists of energy constrained sensor networks that capable of embedding transmission, sensing and processing. This leads to short lifespan and hence the energy efficiency techniques are highly desirable for WSN. Many fields implement WSN with Coverage and Connectivity, one such example is environment data collection. Here a research scientist will collect several sensor readings over a period of time. The collected data gives the trend for analyzing anomaly. Sensor nodes placed at fixed location in an environment perform Security Monitoring and Node Tracking to detect anomaly.

Intrusion Detection System (IDS)

Intrusion detection system (IDS) is a mechanism for detecting intruders based on anomalies, alert users of an intrusion incident, and tries to reconfiguring the network if possible. These malicious intruders can even damage the important information in WSN while transmission. The IDS enabled network will respond and even isolate the intruder thereby guarantee its normal operation.

IDS in WSN

• Within a sensor network it is not possible to have an active full-powered IDS agent inside every node. Each node is usually managed by a human user and is independent from one another.
• Threats can damage and consume large quantity of energy for monitoring nodes that are suspicious without an IDS.
• Low cost and devices within a WSNs are deployed into an open and unprotected area leads to various types of attacks.
• Utilization of network's energy by malicious nodes reduces the life time of network.

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 such as clock-gating, voltage, and frequency scaling, or SW-based. In the context of networked embedded systems, it is known that communications play a vital role in energy consumption and, for this reason, energy efficient transmission strategies have been designed recently. While energy overhead can be tolerated during an attack, it represents a waste of resources when the attack is not active. Therefore, the most important issue to optimize system resources is *intrusion detection*. Traditional anomaly-based intrusion detection systems (IDSs) monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network, what sort of bandwidth is generally used, what protocols are used, and what ports and devices generally connect to each other. Even if applied to control applications traditional approaches look for "formal" or "network-oriented" anomalies and do not analyze the content of packets from the point of view of a control application. For example, altered commands transported by a formally correct protocol are not detected by

traditional IDS. In the context of control systems, some attacks have been designed to be virtually undetectable.

Intrusion detection always been an open problem in Wireless Sensor Network system. It is widely accepted that packet deception cannot be detected simply by looking at the control performance since in many cases, injected data are not distinguishable from normal perturbations of the physical plant. The proposed architecture does not rely on a particular detection mechanism but rather it aims at detecting the beginning and end of the attack and reacting against it. Here we propose the packet based *selective encryption* exchanged between source and destination, with a methodology to detect attack based on the comparing of encrypted and unencrypted commands. Selective encryption was used to guarantee to reduce energy consumption in wireless communications. Attack mitigation for countermeasure to be adopted when an attack is detected is also an issue. This technique has the advantage of eliminating damage risks and performance loss; but at the same time, it should detect the attack duration, so as to reduce the resource consumption. In this work, all packets are encrypted under attack except some anchor packets that is used to detect when attack is over. Here we can clearly say that not all packets are equally important. With this findings we can further improve energy by *varying the packet transmission rate* according to the control performance. Intrusion Detection Systems are to be considered a mandatory criteria for safe operation in wireless sensor networks.

Intrusion Detection mechanism currently in place make use of energy prediction in cluster-based WSN. In this approach the malicious nodes are classified based on energy consumption. That is the algorithm first compares the energy prediction results with the actual energy consumption at the node and the resulted malicious nodes will be put in black list. Energy consumption of the sensor nodes will be predicted by the sink node and also collects each sensor node residual energy. The residual energy will be compared by the sensor nodes with their residual energy through a broadcast message. If algorithm detects abnormal energy consumed at a node then the node's ID will be put in a blacklist. Once it is listed in the blacklist it will be omitted from the routing table. One of the drawback of this approach is that in this methodology the only criteria considered for finding the malicious node is the energy consumed by that particular node. This may not be sufficient data to decide a node is malicious or not without considering its past transactions.

So many wireless protocols are using IDS mechanism. These protocols are available with deterministic and statistical latency discussed. Wireless medium may introduce transmission issues, e.g., delay and packet losses, which can affect control performance. In literature, various techniques have been proposed to address these problems. When wires are not present, energy should be supplied through batteries or harvested from the environment in both cases, energy efficiency becomes a strong requirement to guarantee long device life time without human intervention.

The main cause of energy consumption is transmission for instance. To reduce the energy consumption for computation, but the energy consumption for transmission cannot be easily reduced since it strongly depends on application requirements (e.g., transmission range). Therefore, the proposed security approach aims at minimizing the transmission overhead due to encryption. Energy can also be saved by reducing the transmission rate of commands and output measurements when the control performance is above a desired threshold.

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 Network Control System. 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 and asymmetric (e.g., for symmetric encryption is AES and asymmetric encryption is 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; digeng 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. If the content of the message is changed during transmission it does not correspond with the signature and therefore, the receiver detects the attack. The basic assumption is that it should be computationally infeasible to generate a valid signature for a party without knowing party's private key. When symmetric key is used, the signature is named Message Authentication Code. To detect also replay attacks, a counter can be inserted in the signed message. Here the presence of an end-to-end security protocol is considered. Otherwise packet signing and integrity check are performed at controller and plant side while intermediate network devices just relay packets. In this way, a man-in-the middle attack on a tampered network device cannot modify signed data without being discovered.

If the attacker knows the transmission protocol, it is able to understand whether a packet contains a message signature. In this work, we just define a signed message as "encrypted"

deterministic amount of messages to encrypt them. The selective encryption algorithm integrates both the method and stochastic strategy, in order to increase the uncertainty in the process of message selection. The more uncertain the encryption algorithm is, the secure data communication is based on the assumption that sufficient data is encrypted to provide reliable security.

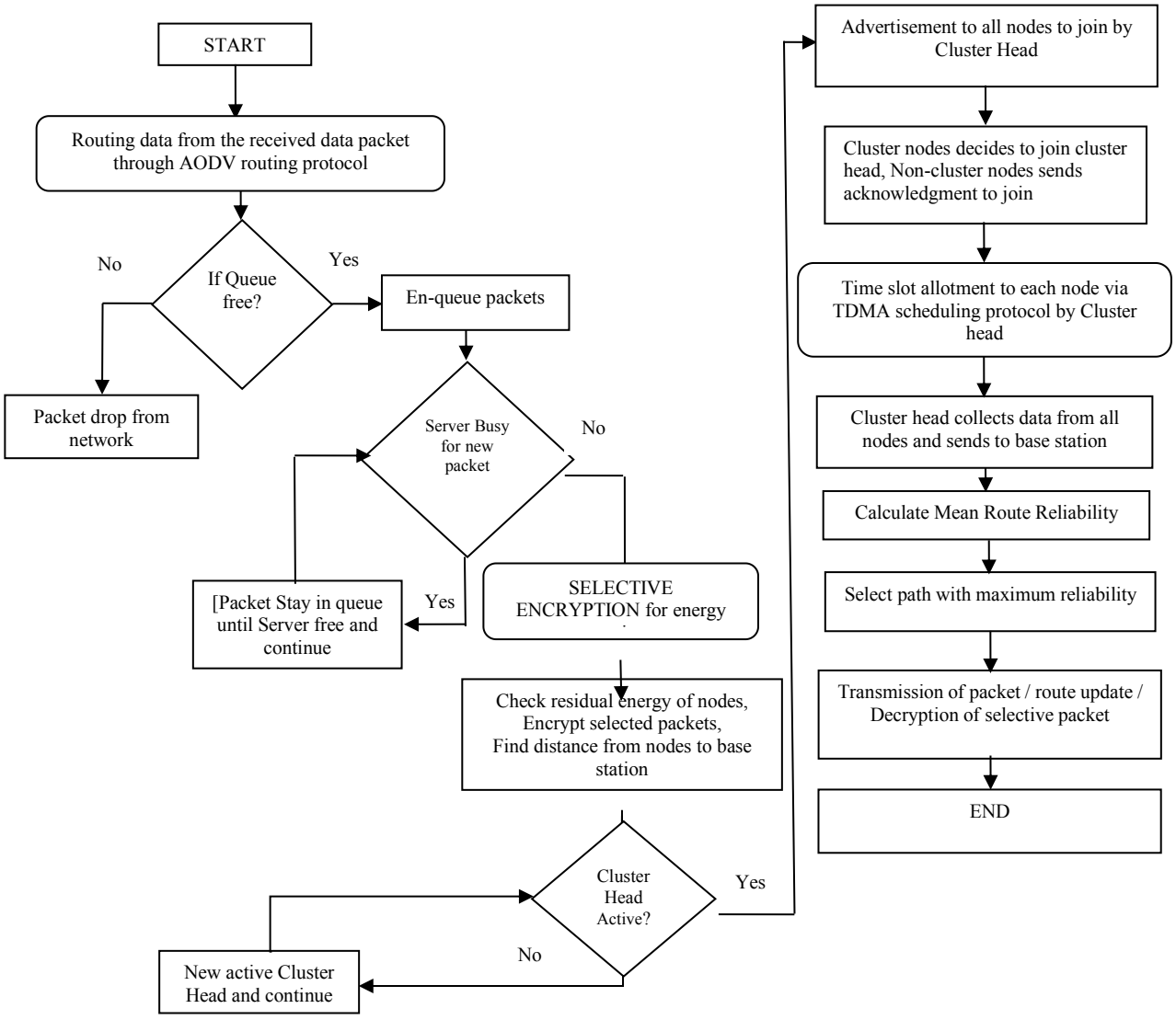

Fig 1. Architecture block diagram of IDS for WSN security

PROPOSED ARCHITECTURE

In this section, we propose an architecture to handle the problems highlighted in the previous section. Fig. 1 shows the block diagram of the architecture.

A selective encryption algorithm aiming to obtain sufficient uncertainty in the system. During the process of sending messages, the sensor will randomly generate a value to indicate the encryption percentage that represents how many messages will be encrypted among the transmitted messages. Then a function is chosen by the sender that is already

IMPLEMENTATION DETAILS

Selective Encryption Algorithm

Selective algorithm is found to be an optimized algorithm for encrypting on selected packets. This comprised of the following three phases:

1) The sender S will first put a random generator RNG to randomly obtain an encryption ratio er. RNG is a computational or physical device that will generate a sequence of number or symbols that cannot be reasonably predicted. It is also important that required security is provided. SR is the Minimum threshold value of

encryption ratio that should be met by the system so as to provide sufficient security protection.

S Sender
er Encryption ratio
RNG Random generator to generate a random, er.
PSR Pre-defined Security requirement of the network system

Representing the relation mathematically,

The sender S has to find out the encryption probability. The job is done through a function Func to generate an encryption probability pi to determine if one message Msg will be encrypted or not.

Where,

2) Following the steps sender selects the messages to encrypt. This improves the uncertainty in the system of which message will be encrypted and which are not. The more uncertainty the more secure the communication.

Following is the algorithm for selective encryption,
Where,

Step 1: Loop through each message from the incoming packets

Step 2: Calculate Entropy of the message under evaluation. The entropy gives a measure of information contained in the message in a logical way.

Step 3: Update Threshold value of message in three below cases.

Case 1: Message under evaluation is the First message Then Threshold value of message should be equal to Entropy

Case 2: Message encryption percentage is less than 50 p.c. Then Threshold value of message should 10p.c. of the current threshold subtracted from previous calculated threshold value.

Case 3: Message encryption percentage is higher than 50 p.c. Then Threshold value of message should 10p.c. of the current threshold added from previous calculated threshold value.

Step 4: Message should be encrypted if the Entropy of the Message is greater than or equal to threshold value of the message. Otherwise, message will not be encrypted.

Step 5: Find out the Encryption percentage.

Step 6: Continue till all messages in the queue is processed.

The above mentioned algorithm improves the uncertainty of the encryption and improves the security by making the attacker to decrypt and decode the message for the use. Entropy of each message give a measure of information contained in each message. In selective encryption if we encrypt messages that have higher entropy then security is reduced. The algorithm tried to selectively encrypt messages having higher entropy and pass messages having low entropy without encryption. Passing messages having lower entropy without encryption increases security of transmission when compared with normal selective encryption. This is so because when the transmission is intercepted; only that part of the transmission is accessible which has lower entropy and other higher entropy parts are encrypted.

II. CONCLUSION

In this paper, we proposed architecture for an energy-efficient security-concern wireless control system. The intrusion and normal disturbance is hard to distinguish at destination side. For battery-powered devices, encryption-based packet protection is energy-consuming. Selective encryption is a mechanism to save energy and to detect attack as well. The appropriate algorithm for Selective algorithm is also discussed in the paper. The selective encryption algorithm along with Clustered network improves the overall security and also lower energy consumption of the final system. The block diagram of proposed system gives the idea that, the adapted encrypted packets according to the attack incident so as to reduce energy consumption. We also proposed to adapt transmission rate to instantaneous control performance since packet transmission consumes energy.

Simulation results also shows that this technique reacts to attacks. Fig 2, shows the graph, generated for Energy consumed (in Jules) against node operation over a period of time. The energy consumption in the proposed system

(below line in graph) is lesser than the existing system (above line in graph). Over the period the proposed system shows 25 p.c. savings of power consumption.

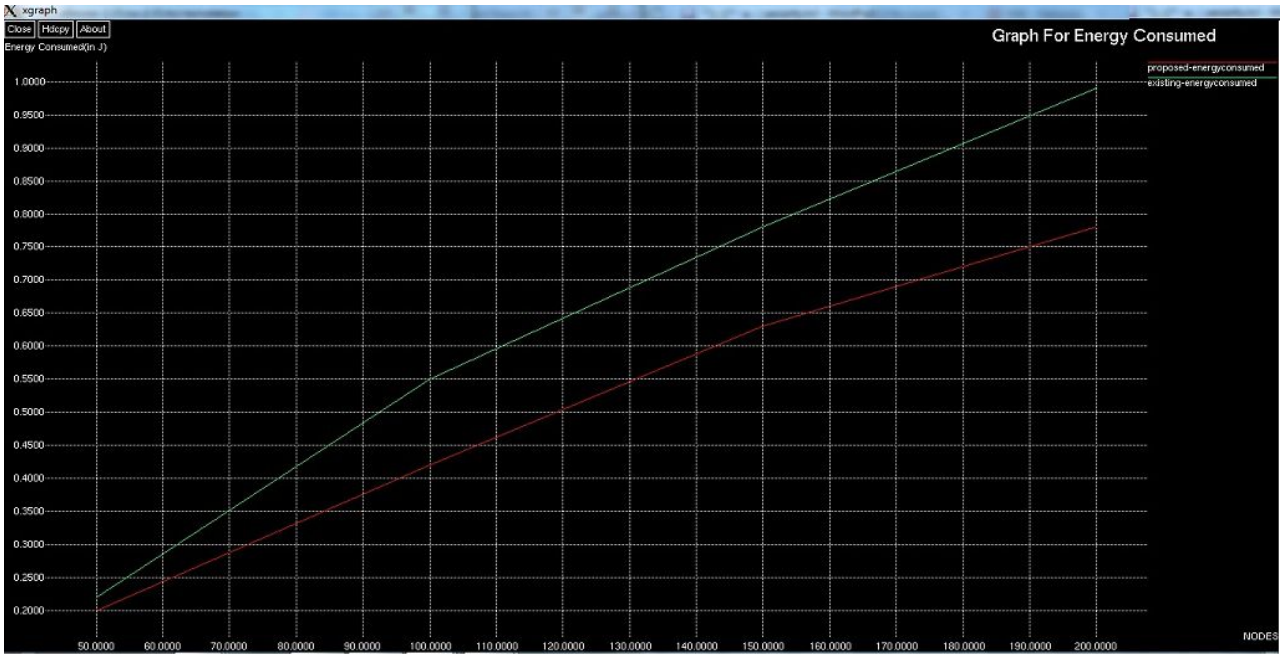

Fig 2: Energy Consumption of Nodes comparing Proposed and Existing System

REFERENCES

[1] IEEE Standard for Local and Metropolitan Area Networks–Part 15.4:Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1:MAC Sublayer. IEEE Standard 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011), Apr. 2012, pp. 1–225.

[2] A.-A. Ahmadi, F. R. Salmasi, M. Noori-Manzar, and T.A. Najafabadi, "Speed sensorless and sensor-fault tolerant optimal PI regulator for networked DC motor system with unknown time-delay and packet dropout,"IEEE Trans. Ind. Electron., vol. 61, no. 2, pp. 708–717, Feb. 2014. [13] A. A. Ghorbani, W. Lu, and M. Tavallaee, "Network Intrusion Detection and Prevention: Concepts and Techniques", 1st ed. New York, NY, USA:Springer, 2009.

[3] P.P.Joby, P.Sengottuvelan, "On the construction of virtual topology structure for secure routing in wiresless sensor Networks", Sensore Letters Vol. 13, 946-952, 2015.

[4] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent resultsin networked control systems," roc. IEEE, vol. 95, no. 1, pp. 138–162, Jan. 2007.

[5] J. Hirai, K. Tae-Woong, and A. Kawamura, "Practical study on wirelesstransmission of power and information for autonomous decentralized manufacturing system," EEE Trans. Ind. Electron., vol. 46, no. 2,pp. 349–359, Apr. 1999.

[6] S. Hussain, M. Mokhtar, and J. M. Howe, "Sensor failure detection,identification, and accommodation using fully connected cascade neuralnetwork," IEEE Trans. Ind. Electron., vol. 62, no. 3, pp. 1683–1692, Mar.2015.

[7] P.P.Joby, P.Sengottuvelan, "A Localised clustering scheme to detect attacks in wireless sensor Networks", International journal of electronic security and digital forensics Vol. 7, No.3, 2015.

[8] Y. Mo, J. P. Hespanha, and B. Sinopoli, "Resilient detection in the presence of integrity attacks," IEEE Trans. Signal Process., vol. 62, no. 1,pp. 31–43, Jan. 2014.

[9] Y. Mo et al., "Cyber–physical security of a smart grid infrastructure,"Proc. IEEE, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[10] S. Pallapothu and S. Mahajan, Selective Encryption Support in SRTP.Fremont, CA,USA: Internet-Draft-smahajan-SRTP-selective encryption-01.txt, IETF Secretariat, Feb. 2007.

S. U. Rehman, K. W. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios," IET Commun., vol. 8, no. 8, pp. 1274–1284, May 2014.

[11] L. Repele, R. Muradore, D. Quaglia, and P. Fiorini, "Improving performance of networked control systems by using adaptive buffering," IEEE Trans. Ind. Electron., vol. 61, no. 9, pp. 4847–4856, Sep. 2014.

[12] T.Poongodi, M.Karthikeyan, "Comparative analysis of DSDV, AODV and DSR for Mobile Adhoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering Vol 6, Issue No. 2, 576-580, February 2016.

[13] P.P.Joby, P.Sengottuvelan, "A survey on threats and security schemes in wireless sensor Networks", International journal of engineering research and applications Vol 5, Issue 1, PP 89-94, 2015.

P N Prajitha, has completed her B.E from Calicut University 2007-2011 and PG scholar in PPG Institute of Technology, Coimbatore under Anna University

T. Poongodi M.Tech, (Ph.D) working as Assistant Professor in Department of Computer Science and Engineering, PPG Institute of Technology Coimbatore-35