Improved Adaptive Acknowledgement Scheme For Intrusion Detection System In Adhoc Through SCADA

G.Dharma prabha
PG Scholar, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology
Coimbatore,Tamilnadu-India

M.Revathi
Assistant Professor, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology
Coimbatore,Tamilnadu-India

***Abstract*— The critical infrastructure provides the predominant problem and more complexity in network. In this paper, we propose a (SCADA-IDS) Supervisory Control and Data Acquisition method to control the complexity in MANETs. The Multi-layer architecture and Multi-attributes are used to implement a new intrusion detection named Improved Adaptive Acknowledgement (IAACK) scheme in ad-hoc network to prevent our network from the internal malicious behavior of the nodes and external attacks. Dynamic features of MANETs make vulnerable to different types of attacks. In this paper, we use some enhanced methodologies and techniques to mitigate varied cyber attack threats in certain circumstances, without greatly affect the network performance.**

Keywords- Supervisory Control and Data Acquisition (SCADA), Intrusion detection system (IDS), Improved Adaptive Acknowledgement (IAACK) scheme, Mobile Ad-hoc Networks (MANETs).

I. INTRODUCTION

The increased complexity and inter- connectivity of the Supervisory Control and Data Acquisition system plays a Significant Role in MANETs. The critical infrastructures largely make use of ICT technologies. In this paper, we present a SCADA Intrusion Detection System tailor-made for identifying the external complex attacks which might interfere with the state of an entire SCADA installation. MANETs is divided into two types namely, single hop and multi hop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi-hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named IAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. In any network there are three crucial aspects of security that may be threatened due to these vulnerabilities: confidentiality, integrity, and availability. An IDS module is used to monitor the system security was successfully implemented in this network.

A. SCADA-IDS:

SCADA system is mainly used for to protecting our systems from external intrusions or malicious attacks. Intrusion Detection System can be used to detect the various malicious behavior of the nodes that can compromise the security and trust of a computer system.

B. IAACK:

The (IAACK) Improved Adaptive Acknowledgment Scheme for protecting our nodes against from internal malicious actions. IAACK can be mainly divided into three parts, namely AACK, S-ACK and MRA. These three techniques are used to detect the malicious nodes behave gently. AACK greatly reduce the network overhead compared to TWOACK. Misbehavior Report Authentication (MRA) can immediately generate the report if any malicious node compromises the gentle node. The S-ACK mode is based on the TWO ACK scheme. For every three consecutive nodes along the transmission route, the third node is required to send back an S-ACK packet back to the first node to confirm receiving the packet.

II. RELATED WORK

First, Yichi Zhang, Ling feng , Wang [3] proposed a Support Vector Machine (SVM) and Artificial Immune System (AIS) to detect and classify malicious data and possible cyber-attacks. AMs at each level are trained using data for supporting the optimal communication routing and improving system security through the identification of malicious network traffic.

Zouheir Trabelsi and Khaled Shuaib [5] proposed ARP cache poisoning attack against other hosts in the network. ARP caches suspicious host in order to force it to forward to the Test host the packets received from its victim hosts.

Elhadi M. Shakshuki [2] proposed Enhanced Adaptive Acknowledgement Scheme (EAACK) to detect malicious behavior nodes and also solve Watch dog problems like 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior report, 5) collusion and 6) partial dropping.

Based on TWOACK, Sheltami et al. [16] proposed a new scheme called AACK. AACK significantly reduce network overhead while still capable of maintaining or even surpassing the same network throughput by using the end-to-end acknowledgment scheme.

Elhadi M. Shakshuki [2] proposed EAACK scheme to implement both DSA and RSA. The goal is to find the most optimal solution for using digital signature in MANETs. EAACK requires digital signature at all acknowledgment process, it still manages to maintain lower network overhead in most cases.

III. PROPOSED WORK

In the existing system, IDS requires data packets to be encrypted before they are sent out and verified until they are accepted. To address the problem of extra resources required due to the introduction of security in MANETs we adopt a security in our proposed scheme to achieve the goal of finding the most optimal solution for using security in MANETs.

A. Multilayer cyber-security framework architecture:

The proposed work in Fig:2 uses SCADA- specific IDS and IAACK scheme to prevent our network environment from the internal and external intrusions or malicious attacks. Multi-layers are i) Enterprise level ii) Substation iii) SCADA level. Enterprise level consists of the enterprise server such as proxy, web, E-mail server. Enterprise level can have a corporate network and corporate demilitarized zones. Control center DMZ containing the inter control communication protocol server and virtual private network (VPN). Firewalls and IDS can be used to detect the incoming traffic. DMZ mean network segment contains the "Security Buffer Area" between the internal and external network. Data center and protocol gateway is used to collect and translate data to different IEDs. Perimeter defends against attacks from exterior enclaves.

B. Multi-attributes ids for SCADA:

The proposed hybrid intrusion detection method consists of three attributes: 1) access-control white-lists; 2) protocol-based white-lists; and 3) behavior-based rules.

a) Access Control White-lists: The access-control white-list approach contains detectors in three layers that is, source and destination medium-access control (MAC) addresses (and) in the Ethernet layer, source, and destination IP addresses (and) in the network layer, and source and destination ports (and) in the transport layer. The detector will take a pre-defined action, for example, it will alert in IDS mode and log the detection results.

$$\mathrm{AC} \notin \{\mathrm{AC}_{\mathrm{wl}}\} \rightarrow \mathrm{Actions}(\mathrm{alert}, \mathrm{log}) \qquad (1)$$

(1)Represent the corresponding white-list set.

b) Protocol Based White-lists: The protocol-based white-list method is related to the application layer (up to layer 7) and deals with various SCADA protocols, such as Modbus, DNP3, IEC 60870-5 series, ICCP, IEC 61850, and proprietary protocols. It can support specific protocols. IDS is deployed at the network between two control centers, the protocol-based detector only allows communication traffic complying with specific protocols; otherwise, it will generate an alert message.

c) Behavior Based Rules: Behavior based detection approach finds and defines normal and correct behaviors by deep packet inspection (DPI).This may include the analysis of a single packet or multiple packet together. In different scenarios SCADA-IDS may have different rules in terms of normal behaviors. SCADA- IDS record the detection results in log file and display the results in Graphical User Interface (GUI) provide the display detection performance and results.

C. Improved adaptive acknowledgement (IAACK) scheme:

In proposed work, IAACK scheme is implemented in the SCADA-IDS to detect the different internal malicious actions and it can be mainly used for the internal communication process. DSA and RSA algorithm are proposed in the IAACK scheme. The SCADA-IDS includes the following modules are: Protocol Extractor, Packet Storage, Flow lookup table, Event Generator, Plug-in-Queues, and Event Controller.

In this IAACK scheme, we implement the hybrid cryptography techniques for reducing the network overhead. IAACK consists of three major parts namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). By using Digital Signature Algorithm (DSA), all acknowledgment packets are required to be digitally signed by its sender and verified by its receiver.

a) ACK and S-ACK SCHEME: ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in IAACK, aiming to reduce network overhead when no network misbehavior is detected. In Fig. 1, in ACK mode, node S first sends out an ACK data packetPad1to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order. Within a predefined time period, if node S receives Pak1, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

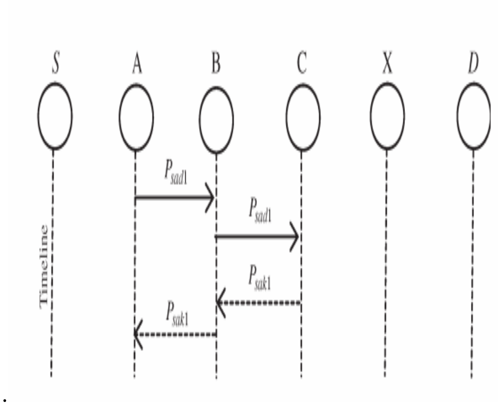

Fig:1 ACK and SACK : The destination node is required to send back an acknowledgment packet to an source node when it receives a new packet.

b) MRA: The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious by adopting an alternative route to the destination node, When the destination node receives an MRA packet, it searches its local knowl-edge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whenever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.

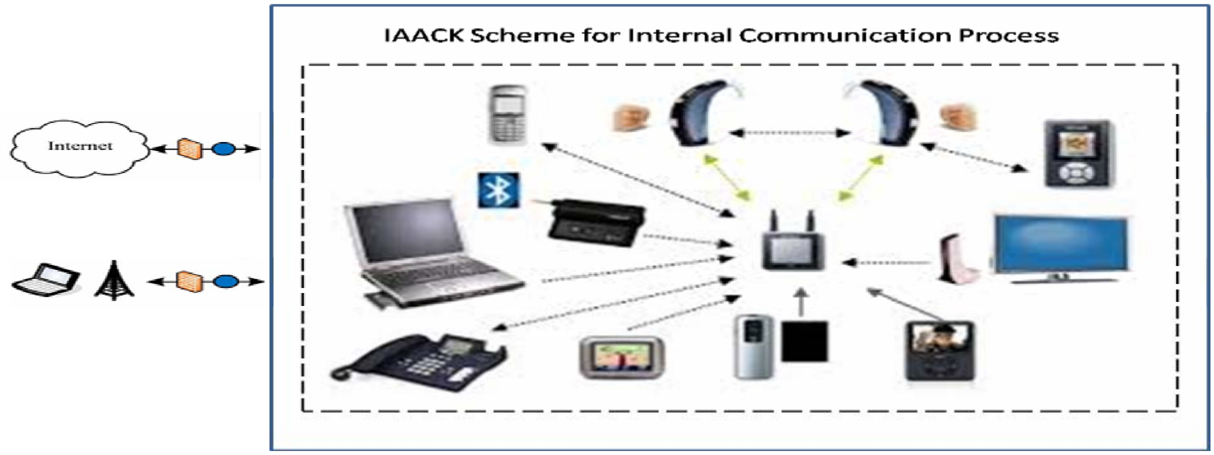

Fig:2 IAACK SCHEME AND SCADA-IDS applied for Internal and External Communication Process.

D. Digital signature:

IAACK is an acknowledgment-based IDS. All three parts of EAACK, namely ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. IAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. We implemented both DSA and RSA digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

IV. CONCLUSION

This paper has presented a layered cyber-security framework for SCADA systems which combines security enclaves, IDS technology, and behavioral monitoring to make SCADA systems more secure. The framework provides a hierarchical approach for an integrated security system, comprising distributed IDSs. Packet dropping attack has always been a major threat to the security in MANETs. We proposed a novel IDS specially designed for MANETs and compared it against other popular mechanisms in different scenarios. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attack. The proposed algorithm is very efficient and less complex compared with other techniques. Eventually scheme is more suitable to be implemented in MANETs.

REFERENCES

[1] G. 1. Y. Yang, K. McLaughlin, S. Sezer, T. Littler, B. Pranggono and H. F. Wang, "Multi-attribute SCADA-Specific Intrusion Detection System for Power Networks" IEEE Transaction on power delivery L.29, NO. 3, June 2014.

[2] Elhadi M. Shakshuki, Nan Kang, and Tarek R.Sheltami,―EAACK—A Secure Intrusion-Detection System for MANETs IEEE Trans .Ind. Electron, Vol. 60, No. 3, pp.1089-1098,Mar. 2013.

[3] Z. Yichi, W. Lingfeng, S. Weiqing, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids,"IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[4] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detect ingintrusions in SCADA systems," IEEE Trans. Ind. Inf., vol. 7, no. 2, pp.179–186,May2011.

[5] Z. Trabelsi and K. Shuaib, "Man in the middle intrusion detection," in Proc. IEEE Global Telecommun. Conf., 2006, pp. 1–6.

[6] I.N.Fovino,A.Carcano, T.DeLacheze Murel,A.Trombetta,and M. Masera, "Modbus/DNP3 state-based intrusion detection system," inProc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl., 2010, pp. 729–736.

[7] [3] K.Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, ―Which wireless technology for industrial wireless sensor networks? The development of OCARI technol, IEEE Trans. Ind. Electron. vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[8] 8. R. Akbani, T. Korkmaz, and G. V. S. Raju, Mobile Ad hoc Network Security, in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[9] R. H. Akbani, S. Patel, and D. C. Jinwala, ―DoS attacks in mobile ad hoc networks: A survey, in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012,pp.535–541.

[10] R. H. Akbani, S. Patel, and D. C. Jinwala, ―DoS attacks in mobile ad hoc networks: A survey, in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012,pp.535–541.

[11] G. Jayakumar and G. Gopinath, ―Ad hoc mobile wireless networks routing protocol—A review, J. Comput. Sci., vol. 3, no. 8, pp. 574–582,2007.

[12] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks", in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[13] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs", in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10,2010, pp. 216–222.

[14] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs", in Proc. IEEE 25th Int. Conf. AINA, Biopolis,Singapore, Mar. 22–25, 2011,pp.488–494.

[15] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator,"IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[16] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

[17] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1983.