International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Trust System for SCADA Network Using Wireless Sensor Based on Node Behaviors

B.Padmini[1], N. Chandra Shekar Reddy[2], Ch. Mukunda Reddy[3]

[1]Student, M. Tech CSE Department, Institute of Aeronautical Engineering, Hyderabad-500043, Andhra Pradesh, India,

[2]Professor, CSE Department, Institute of Aeronautical Engineering, Hyderabad-500043, Andhra Pradesh, India

[3]Assistant Professor, CSE Department, Institute of Aeronautical Engineering, Hyderabad-500043, Andhra Pradesh, India

Abstract: ***This paper discuss about the communication security device called a trust system through wireless sensor network based on node behaviors. The major goal of the trust system is to increase the security efficiency compared to firewall and also apply a novel trust evaluation algorithm defined a NBEA (Node Behavior Evaluation Algorithm).This paper concentrates on placing the trust system at the border context which creates anew trust system that increases the flexibility and also demonstrates the trust system using TCP/IP router. The main discuss in the following ways: 1) Summarizes the major threats against SCADA systems.2) Discusses about the new trust system which implements a wider array of network enabled equiqment.3) Impact of the trust system through TP/IP network communication between node and other behaviors. 4) As wireless sensors network are being vulnerable and to be attacked and also compromised. In order to avoid network problem a trust evaluation algorithm is defined as NBEA (Node Behavior Evaluation Algorithm) proposed, which integrate behavior strategy.***

Keywords: supervisory control and data acquisition (SCADA) systems, Node Behavior Evaluation Algorithm (NBEA)

1. Introduction

A trust system is a security device with a firewall and detection capabilities designed to use at the time-critical network system. A trust system can perform real-time requirements that the supervisory control and data acquisition network TCP/IP and UDP/IP communication. A secure system requires all existing devices be replaced and also implemented in existing utilities. Trust system uses an network routing architecture that allow utilities to communicate with the system without requiring the upgrade. This article places the trust system at the boarder that have appeared in related work and also followed by , how this trust system help to address such concerns.

The Internet-protocol (IP) standards and common operating system (windows, UNIX) SCADA system is being vulture by the attackers who are familiar with IP-based techniques downloaded from Internet. The original trust system had only active mode router. This paper introduces passive mode, half active mode and tunnel gateway mode. In advance tunnel gateway node, the TCP/IP communication is done between the systems trough TCP/IP communication protocols. As the wireless sensors networks which are flexible, accurate and inexpensive and also easy to deploy. So, this article applies this wireless sensor network technique to this gateway mode. But as the node is vulture, to be attacked by eave dropping etc.

We propose NBEA algorithm by which firstly each node establishes direct and indirect trust values of the neighbor nodes with various trust factors. The trust factors include packet receive, delivery etc.

2. Literature Work

2.1 Supervisory Control and Data Acquisition Overview

SCADA central and distributed system monitors and controls a single site [1]. These systems are found through the public utility industry such as air traffic control, electric power generation [4]. Due to the sensitive nature of the SCADA system attacks may be directly (or) indirectly, in the financials and data loss.

Threats:

1. Threat Source:
   Industrial sources for cyber attacks may be Industrial Technical design error, natural disaster and also operational error.
2. Specific Treats:
   Mainly in the business and engineers is incredulous, lack of resources and also technical issues to plan and maintain security upgrades that reduces the profit.
3. Real World Incidents:
   There are several real-world incidents that are affecting the SCADA systems [4].

1) In 2003, the Slammer worm took Ohio's David- Beese nuclear power safely to monitor offline for five hours [4].
2) In 2001, hackers hacked CAL-ISO California primary power grid operator.

2.2 Changes in SCADA Environment:

The restricting of utility had increased while driving the need in more efficient and better utility coordination. The first element is the regulatory. The second element is changes made in large-scale operations of grid. Restricting can be done incrementally And finally, In early stages , large utilities are to be owned beginning-to –end power production and were broken into smaller companies for only transmission or distribution.

2.3 Current SCADA System Protection

The old architecture is to install a system, run it unattended and can be replaced I five years or more. The new PC based systems utilities were copied for more dynamic operating based system, without impacting 24/7/operations [4]. On the positive side, the consistency of the SCADA is becoming increasing day by day, vulnerabilities and there increased emphasis on SCADA information system is being secured. National laboratories had performed many tests on the SADA security.

Conventional IT security approaches focuses on the standalone products such as firewalls, router ACL's etc associated with the individual network devices. In this point-oriented approach is vulnerable to attack the environment that circumvents only one particular security control. Coordinated security paradigm is needed to take the advantage over the capabilities of the devices such as routers and also the large-scale network activities.

In the future, the power grid will begin to support the high level of the interaction and also the federated system services. The trust system concept supports the goals from the current and the future SCADA system. These goals also include the ability of self-healing, dynamic and predictive rather than reactive, distributed terms of the information that is able to do increase system security.

Firstly, in former system, the individual trust system is to collect the authorized information from other ones. The trust chain exists between the two strange individuals. But this was said to be very dangerous. Secondly, the latter system individuals require all kind of related information, interacting rules and also the individual opinions. Finally the sensor nodes are obtained by the other nodes of the trust values.

Viljanen, came up with all kinds of ingredients of trust evaluation after nearly ten years of research on the trust of the network, which has guiding effect on the trust measurement of the sensor node in wireless sensor networks. Crosby et al, purpose a trust evaluation model based on the classical probability considering the trust recommendation between sensor nodes; therefore it cannot reflect nodes real-time trust state accurately. Ganeriwal et al, make a trust evaluation model and uncertainty analyses based Bayes theory. Because the lack of prior knowledge about wireless sensor networks, the model subjective assumptions of prior distribution aggravates is the uncertainty of the trust system. Tang et al, purposes a trust system evaluation based on the fuzzy logic that provides formalized mechanism and also a specific trust calculation.

3. Trust System

3.1 Future Intranet

Many researchers conformed that Intranet is like a utility that was also said to be like internet .SCADA is likely to migrate to the future intranet to increase the bandwidth availability .The new environment present an extreme challenges to the internet are almost to exit, including in the issue of cyber attacks. The new industries turning to next-generation increases demand exchange is the power grid. The latest utility is said to be the grid efficiency. The future intranet is also used to provide the improvement in protection and also control of utility. The introductions have many benefits such as increased information sharing, protection and also the control on grid. Care is taken on network capabilities, security and also communication protocols to meet the requirements. IT system and SCADA system focuses on different information priorities .These IT system priorities are integrity, confidentiality, availability of SCADA system provide personal safety and product quality safety. Now these SCADA and corporate IT system develops security mode. Currently the dial-in modems connect to one system compromising others, these are unprotecting, internet connection exposing the SCADA network provide 24/7 operations. Through this future interaction, these SCADA system network maintains the same level of service that is required by customers depending on the IT security mechanism on the top of SCADA network without unique requirements.

3.2Trust System Concept

3.2.1 What is trust system?

This concept is to provide non-proprietary system; in this the software agent's plug into a existing network to proper function of correlating data and also identify risk levels. The trust system is a software agent performing security analysis and response. In a network where nodes acts as the interface between incoming message and also between nodes.

3.2.2 What these trust systems do?

This system reacts to the status messages and also comments from network nodes. For some companies the legacy SCADA nodes and the legacy SCADA nodes and the other type of communication requirement require protocol gate way plug-ins and analysis packet delivery. The trust system validates identifier risk, bad data and also the input these assigns data-type for good data element .It next determines is authorized to read all data types in messages that were received from the recipient. If the message neither are nor authorized then the message are deleted from which recipient they were sent .Finally, only good data are said to transferred to the database and the unprotected data is not allowed to enter into the database. So, by this the protection of the databases is more and more given priority, so that is cannot be attacked.

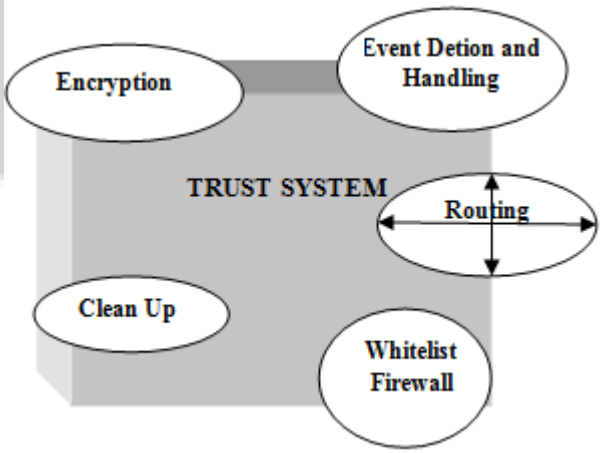

Figure 1: Trust System Capabilities

3.3 Trust System Implementation

3.3.1Implementation

Trust system can be implemented in many ways, this is said to be the main strength of the trust system, and this trust system can be implemented on the current architecture. Since every company network will be different, so each individual company has its own individual network and also determine financial feasibility to identify their weak points. These trust system is cost efficient and also well suited for meetings.

a) Passive mode Implementation:
In this mode, the device connected to a hub that links between the SCADA control station and the nodes that controls between the company's SCADA network and also the outgoing connection to the rest of the Internet. In this passive mode, system sniffs packets as they pass and also saves the copy to analyze and also alerts if the security is failed .The advantage of this mode is that the in- line with communication.

b) Half active mode Implementation:
In this mode the implementation of blocking with a passive mode is for the trust system to interact with a separate firewall or any router access control lists that blocks future packets by the source of internet protocol that acts as interface, transport protocol and also many message type combinations .The main advantage is that the passive monitoring will be combined with a way to halt the malicious traffic.

c) Active Mode Implementation:
This article mainly experiments the used trust systems in the active mode that shows the blocking functionalities. A trust system is said to be the active mode where hardware is the line with all the communication between SCADA network and any connection to the rest of the intranet. This device mainly said to be specialized trust-box which is responsible for all the routing packets .The main aim of this design is to able to attack the other potential harmful denied entry that is added to the firewall rules. Access Control Number is set for a specific user. The main disadvantage is it is a single point of failure, if the trust system fails this cannot be any alternative.

d) Tunnel (or Gateway) Mode Implementation:
In this case node s cannot be loaded with node trust agents and also the CPU cycles for encryption, this system can be implemented either in passive or active tunnel mode.

e) Advanced Tunnel (or Gateway) mode for wireless:

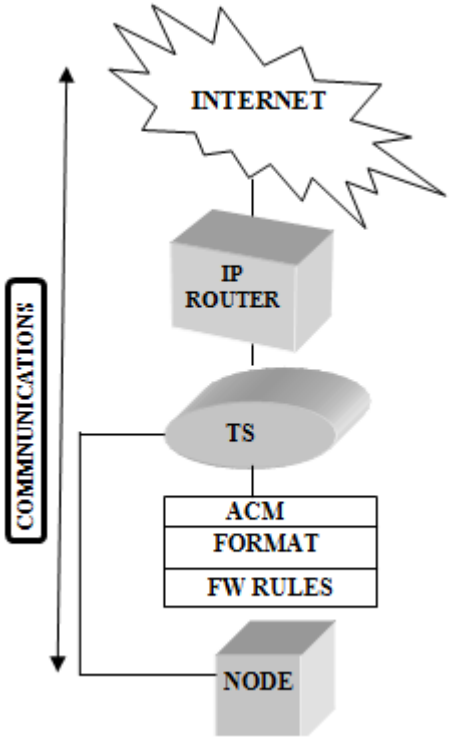

Figure 2: Advanced Gateway Tunnel

Fig 2 shows the architecture of the gate way tunnel that uses the IP router. Instead using multiple Trusted Systems, only one trusted system is used in wireless. The connection takes place trough IP router between the trusted system and internet. This can also be taken place between different trusted systems. The main advantage of this architecture is, many number of trusted systems need not be placed. So that only one trusted system is enough.

4. NBEA Node Behavioral Evaluation Algorithm

NBEA algorithm establishes various trust factors that depends on the interaction between the neighbor nodes. The trust values are obtained by the combining network security degree and correlation of time. It apples fuzzy set theory that measures how mush trust value of the node belongs to the trust degree. The integrated trust value considers several neighbor node recommendations the trust difference between the several evidences.

4.1 Trust Evaluation between Neighbor nodes:

Trust factors depend on a evaluation nodes and also on the third party recommendations. In the wireless network features the trust evaluation mechanism without central node, where neighbor nodes monitor each other. This article consists of the objects of the trust values of both direct and also indirect trust values. The Fig 3, shows that node *j* is said to be subject, which not only makes direct assessment which object *i*, these also makes indirect assessments with objects *i* through nodes *g1, g2, g3*

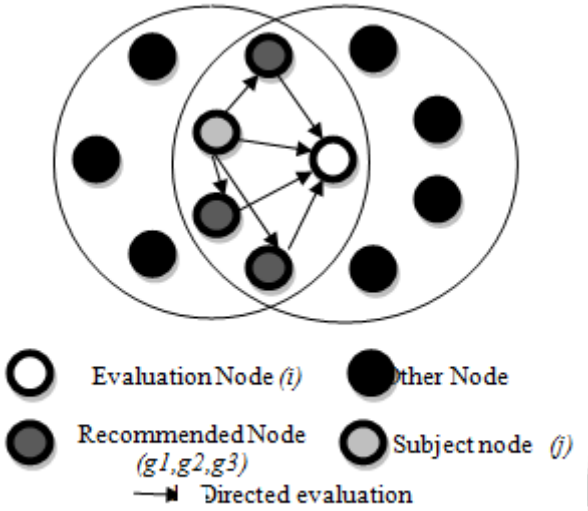

Figure 3: Trust Relationship Between Nodes

4.2 Trust Factors

It is essential to make quantitative and qualitative analysis of various factors which affect trust value in order to evaluate a node's trust worthiness. In the following, We assume that node *i* makes trust evaluation for node *j* and ACK mechanism is adopted. In other words, once the node receives a packet, it sends ACK feedback information to the sender.

1) The factor of received packets rate $RPTF_{i,j}(t)$: According to the assumption, if node *i* monitors node *j* to confirm how many common ACK packets node *j* sends, the ratio of packets received by node *j* can be obtained. According to the change of the ratio, we can know whether node *j* has response forging behavior. If the change maintains in the interval $(-\xi, \xi)$ in different periods, node *j* works normally. The calculation equation is as follows ($RPT_{ij}(t)$ represents the number of received packets):

$$RPT_{ij}(t) = \frac{RPT_{ij}(t) - RPT_{ij}(t-1)}{RPT_{ij}(t) + RPT_{ij}(t-1)}$$

2) The factor of successfully sending packets rate $SPR_{i,j}(t)$: Assume that *j* sends packets to *k* who is beyond the communication scope of *i*. Although *i* cannot monitor the successfully sent packets rate of *j* directly in this situation, node *i* can monitor the number of the same packets sent by *j*. It's known that every packet sent by nodes contains a time stamp and can be distinguished efficiently even if the packets have the same content. Thus, we can obtain the sending number of a certain packet according to different time stamps. The equation as follows ($SPR_{ij}(t)$ is the needing number of sent packets, $SFR_{ij}(t)$ is the repeating number of sent packets):

$$SPR_{i,j}(t) = \frac{SPR_{ij}(t)}{SPR_{ij}(t) + SFR_{ij}(t)}$$

3) The rate of data forwarding $TPFR_{i,j}(t)$: Multi-hop is usually necessary since most of nodes are impossible to communicate with the base station directly. If node *k* is beyond the communication range of node *i* and sends data packets to node *j*, node *i* cannot monitor the received packets number of node *j* directly and has to collect the ACK feedback information of node *j* to obtain the number of received packets. In order to distinguish the forwarding packets and the remained packets, an ACK packet which contains a special bit is constructed. Once node *j* receives a forwarding packet, it broadcasts an ACK packet above. Then node *i* can collect these ACK packets of node *j* to obtain the number of forwarding packets. According to the change rate of $TPFR_{i,j}(t)$, it can efficiently avoid Sinkhole attack and Sybil attack, as well as identify whether the node is selfish. The equation as follows ($FPR_{ij}(t)$ is the number of transmission packets):

$$TPFR_{i,j}(t) = \frac{FPR_{ij}(t) - FPR_{ij}(t-1)}{FPR_{ij}(t) + FPR_{ij}(t-1)}$$

4) The consistency factor $CPFT_{i,j}(t)$: The data packets have spatial correlation, that is, the packets sent among neighbor nodes are similar in the same area according to the application.. Node *i* acquires a packet transmitted by *j* randomly and makes the comparison with its own data. If the source node of this packet is in the same area of node *i* and the diversity rate maintains in the interval $(-\xi, \xi)$, the number of accordant packets increases. Elsewise, if the source node does not belong to the area of node *i*, the consistency factor between node *i* and node *j* would not be adopted. The $CPFT_{i,j}(t)$ equation as follows ($EPT_{ij}(t)$ is the number of accordant packets, $NEPT_{ij}(t)$ is the discordant one):

$$CPFT_{i,j}(t) = \frac{EPT_{ij}(t)}{EPT_{ij}(t) + NEPT_{ij}(t)}$$

5) Time factor $TFFR(t)$: Trust value has context relationship in time and content, and changes on the previous base. The size of time grade is dependent on the specific situation. If it is established too large, integrated trust value will be affected by history too heavily, which may cause errors in node evaluation. On the contrary, if it is established too small, trust value relies on a single period overly. Above all, we have the rules based on the security degree of networks. When the security degree is relatively high, $TFFR(t) = 0.8$, relatively low, $TFFR(t) = 0.2$, normally, $TFFR(t) = 0.5$.

6) The factor of availability $HPFR_{i,j}(t)$: In some cases, the neighbor nodes are inaccessible due to wireless channel interference or bad environment. Concretely, node *i* sends HELLO packets for the detection whether they can be received by node *j*. If node *i* receive the ACK-HELLO packets from node *j*, it is proved that node *j* is accessible. The $HPFR_{i,j}(t)$ equation as follows ($ACKT_{ij}(t)$ is the amount of packets which have been responded, $NACKT_{ij}(t)$ is the amount of packets which haven't been responded):

$$HPFR_{i,j}(t) = \frac{ACKT_{ij}(t)}{ACKT_{ij}(t) + NACKT_{ij}(t)}$$

7) Security grade SGR: According to specific application environment and scenario, the WSNs require different security degree based on different needs. For instance, there is a large difference between batter filed application and environmental monitor. When security requirement is high, SGR = 3, relatively low, SGR = 1; normally, SGR = 2.

4.3 Simulations

We used Mat Lab as simulation tool to analyze the performances of the NBEA algorithm in this section, which includes: trust evaluation of credible nodes, incredible nodes, and malicious nodes, as well as the influence of factors on the trust evaluation. The concrete simulation scene is a square area of 100 m × 100 m, with 100 randomly deployed nodes. Here the communication radius is 20 m. We assume node *i* is subject node and node *j* is evaluated node, overlapping part of two circles is the common neighbor of evaluation and evaluated node. From the viewpoint of rigorous security requirement, the pessimistic initialization strategy of trust value is adopted, and the initial trust state of nodes is set as incredible. Some parameters vary with the scenes and the purposes of experiment and will be explained in detail.

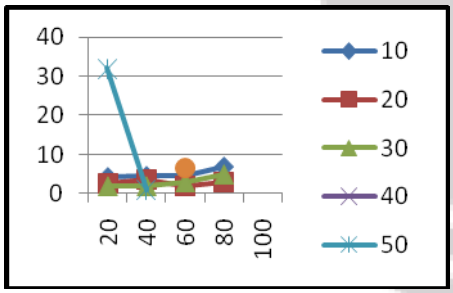

Figure 4: Distribution Map of Random Nodes.

5. Conclusion

SCADA networks are attacked by the digital source as well as by the natural disasters. The proposed trust system is developed with strict requirements to the SCADA network and also providing a secure environment. The explained trust system is flexible and also be implemented according to the SCADA network needs. This trust system is accessed through IP address; in this the secured environment is applied for not assessing the IP addresses. Establishment of the trust factors considers network's practical application environment. At the end the NBE algorithm represents the nodes i.e. the messages are sent trough packets by which data is sent trough the trust system.

References

[1] "A Trust System Architecture for SCASA Network Security" Presented by Gregory M. Coates, Kenneth M. Hopkinson, Scott R. Graham, Stuart H. Kurkowski
[2] "A Trust Evaluation Algorithm for Wireless sensor networks based on node behavior" Presented by Renjian Feng, Xiafeng Xu, Xiang Zhou and Jiangwen Wan.
[3] "Collaborative, trust-based security mechanisms for a regional utility intranet" presented by G. M. Coates, K. M. Hopkinson.
[4] "Quality of service considerations in utility communication networks" K. Hopkinson, G.Roberts, X. Wang

Author Profile

Badarvada Padmini Received B. Tech Degree in the Branch of Information Technology from Sir Catamanchi Ramalinga Reddy College of Engineering from 2004 to 2008. At Present Pursuing M. Tech in the Branch of Computer Science and Engineering in Institute of Aeronautical Engineering. She had also worked as a Software Developer and also an Assistant Professor.