International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.2, Issue No.6, pp : 579-582 1 June 2013

Efficient Cross Layer Mitigation in SCADA Network

S. Thamaraichelvi, N. Rajeshkumar, B. Dineshshankar

Department of Applied Electronics, Sasurie College of Engineering, Tirupur, Tamilnadu, India.

thamuju13@gmail.com, rajeshkumar.n1@gmail.com, dinshan555@yahoo.co.in

Abstract- Almost all the Industrial Data Acquisition and control systems today use connection oriented concepts for interfaces. However, various shapes and functional commands that each cable or wire based system has also raises numerous problems: the difficulties in locating the particular area affected by the industrial parameter, the complexity in operation of the system, the maintenance issue and so on. The control of sensitive industrial parameters by using SCADA-based wireless technology has gained significant industry and academic attention lately for the usability benefits and convenience that it offers users. The control of the temperature of a room containing chemicals and toxic gases the existing research has failed to provide a flexible solution for controlling such conditions by connection- oriented systems. They have used cables and bulky equipment which require large amount of space, high degree of the maintenance and are easily detoriated by moisture and excessive heat. Additionally, the Data acquisition and control techniques used so far have imposed considerable computational burden and have not provided a consistent and accurate results expected by the employees and their industries.

Index Terms:- **SCADA, Cross Layer Mitigation, Wireless Technologies**

I. INTRODUCTION

A wide variety of industrial processes are managed via computerized control systems, and their diverse purposes mean that industrial control systems themselves are diverse in implementation. The term SCADA is most frequently used to describe systems whose assets are highly distributed geographically. The control of power grids and oil and gas pipelines, for instance, involves aggregating sensor measurements from hundreds of widely dispersed field devices so that operators can use a centralized control interface to manage the whole process in real time. Field devices of in the centralized network are located physically close to the portion of the process that must be controlled, and monitor sensors and drive actuators connected to the process.

They are connected to the SCADA control center via a wide area network which may use a variety of topologies and protocols and be wired or wireless.

Such systems with low bandwidth and relative lack of reliability of the networks in use are taken into account, perhaps employing fault-tolerant hardware and algorithms. In addition, they must typically content with legacy hard-ware and protocols since widely dispersed hardware devices are difficult and expensive to upgrade. Much smaller scale operations, such as chemical industries and pharmaceutical processing facilities, are some examples of SCADA systems.

These geographically localized processes may reside entirely within a single plant floor and are sometimes differentiated from geographically dispersed SCADA systems with the term Distributed Control Systems (DCSs). These systems use field devices that are located physically close to the portion of the process under control and are connected to the master control centre via the control network. The control of the whole process is modularized with the use of local controllers to provide fault tolerance and reduce the impact of a malfunction at a single field device.

DCSs typically use a highly reliable and relatively high bandwidth LAN to connect field devices with the control center. In addition, physical security may be more effective since a geographically centralized system is less difficult and expensive to protect. Although the systems that employ SCADA are widely varied in topology, scale, and purpose, they are unified by a single type of architecture.

The recognition of their fundamental similarities is important to the research of SCADA security, since it allows researchers to make use of general models of the class of the class of all SCADA systems. This general model is composed of four major parts: the process to be controlled, the field devices physically connected to it, the centralized control center, and the network that connects the controller and field devices.

A.PROBLEM DEFINITION

Recent research works in WSN have focused on Quality of Service (QOS) support to improve the reliability and performance under severe energy constraints. The improvement of QOS can be tack- led in any layer. For instance several research works has been carried out on improving real time support in MAC sub-layer using GTS (Guaranteed Time Slot) mechanism of IEEE 802.15.4. This improves only real time QOS in single hop networks. In network layer, which provides end to end real time QOS in multi hop networks, this is done by adding and improving the QOS support to the routing algorithm. However, before doing that we need to analyze the performance of the existing routing algorithms. It is clear that our aim in long term is to provide real time support in ZigBee Routing Protocol (ZRP).

The motivation for proposing this analysis is to have a better idea of routing in the ZigBee stack. We believe that this is a good starting point for providing QOS support to ZigBee standard. Actually, the results showed that the HTR algorithm is very interesting for supporting real time communications. So, a first work is made to improve its end to end delay.

B. EXISTING SYSTEM

The AODV routing protocol is a reactive routing protocol; thus the routes are determined only when its needed. Figure 1 shows the message exchanges from the sender to receiver of the AODV protocol.

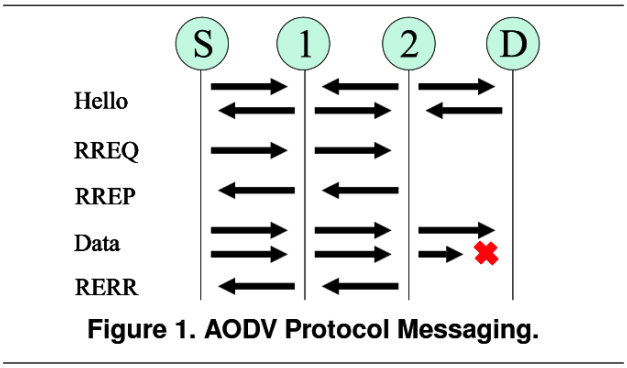

Figure 1. AODV Protocol Messaging.

Figure.1. AODV Protocol Messaging

Hello messages may be used to detect and monitor other neighbor links. Due to the use of Hello messages, each active node periodically broadcasts a Hello message that all its neighbors receive. Because Hello messages are periodically send by nodes, if a node fails to receive continuous and periodical Hello messages from a neighbor, a link break is detected. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when RREQ is received, a route to the source node is created. If the receiving node has not received this RREQ, does not have a current route to the destination, it re-broadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-by- hop fashion to the source. If RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it forms the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. As data flows towards the destination from the source, the timers present in the route nodes updates automatically associated with the routes to the source and destination, by maintaining the routes in the routing table. If a route is not used for period of time, then there will be an oscillation in a node that the route is still valid or not; consequently, the route will be removed from its routing table. If link break is detected, a Error (RERR) is sent to the source of the data in a hop-by- hop fashion. If the error propagates, each intermediate node in the network validates routes to any unreachable destinations. When the source receives the RERR, it validates the route and reinitiates route disco very if necessary.

C.PROBLEMS

The AODV routing protocol provides efficient paths by broadcasting route request (RREQ) messages. However, broadcast to find routing paths consumes much communication bandwidth and might cause a broadcast storm problem. In addition, the routing table for the AODV routing protocol could be a large memory overhead for low-cost ZigBee devices. As the number of route discovery increases, the routing table is depleted and the routing performance rapidly deteriorates.

The major drawbacks in AODV:

- Overhead on the bandwidth: It will be occurred compared to DSR, when an RREQ travels from node to node in the process of discovering the route info on demand, it sets up the reverse path in itself with the addresses of all the nodes through which it is passing and it carries all this info all its way.
- No reuse of routing info: AODV lacks an efficient route maintenance technique. The routing info is obtained including for common case traffic.
- Vulnerable to misuse: Sometimes the messages can be misused for insider attacks including route disruption, route invasion, node isolation, and resource consumption.
- AODV lacks support for high throughput routing metrics: AODV is designed to support the shortest hop count metric. Count metric favors long, low band width links over short, and high-bandwidth links.
- High route discovery latency: AODV is a reactive routing protocol. It does not discover a route until a flow is initiated.

II.PROPOSED SYSTEM

The ZigBee network layer supports all type of network topology. Our study is focused on the performance of HTR topology, only this one will be described. In tree networks, a master device called ZigBee coordinator is responsible for starting the network and for choosing certain key network parameters. The network is then extended using ZigBee routers. End devices can join the network through an association to either the ZigBee coordinator or the ZigBee router. The data and control messages forwarding follow a hierarchical routing strategy. Cluster Tree networks may employ beacon-oriented communication as described in the IEEE 802.15.4 specification. When the tree address allocation is enabled, the network addresses are assigned using a distributed address allocation scheme that is designed to provide every potential parent with a finite sub-block of network addresses to distribute to its children. During network establishment, the ZigBee coordinator determines the maximum number of children per parent (Cm) and the maximum number of ZigBee routers (Rm) between these children. In addition, every node has an attribute called depth which is the minimum number of hopes to reach the ZigBee coordinator using only parent child links. The ZigBee coordinator has a depth of 0 and determines the maximum depth of the network (Lm). A function called Cskip (d) (equation 1) is used after that to calculate the size of the address sub-bloc being distributed by each parent located at depth d.

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.2, Issue No.6, pp : 579-582 1 June 2013

$$Cskip(d) = \begin{cases} 1 + Cm \cdot (Lm - d - 1), \text{ if } Rm = 1 \\ \dfrac{1 + Cm - Rm - Cm \cdot Rm^{Lm-d-1}}{1 - Rm}, \\ \text{otherwise} \end{cases}$$

Network address distribution is as follows. The coordinator has always the address 0. For router- capable child devices, the address assignment uses the value of Cskip (d) as an offset: if the node is the first served, its address is 1 greater than its parent address. Otherwise, the addresses are separated from each other by Cskip (d). For simple end devices, network addresses are assigned in a sequential manner using the following rule:

$$A\,n = A\,parent + Cskip(\,d\,) \cdot Rm + n$$

Here $1 \le n \le (\,Cm - Rm\,)$ and A parent represents the address of the parent.

Routing rules:

If The node has a routing table and there is a routing table entry for the destination
then Use it
else if There is a room for another entry
then Try a route discovery
else Route along the tree using HTR
The route discovery uses a modified version of AODV. The only difference is in the cost of a link. The link cost C { l } for a link l is a function with values in the interval [0 . . . 7] defined as

$$C\{l\} = min\left(7, round\left(\frac{1}{p_l^4}\right)\right)$$

Here pl denotes the probability of packet delivery on the link l. We shall note that the standard permits to report a constant value of 7 for link cost (thus we come back to the standard version of AODV). AODV is a reactive routing protocol; the network is silent until a connection is needed. The network node that needs a connection broad- casts a request to its neighbors who forward this message to theirs and record the node that they heard it. When a node receives a message and already has a route to the desired node, it returns a message through the reverse route to the requesting node. The needy node then search for the least number of hops through other node then it begins using the route. The hierarchical routing is based on comparison rules: for a ZigBee Router with address A at depth d, if the following expression is true, then the destination device with address D is a descendant.
$A < D < A + Cskip\,(d - 1)$

If it is the case, the Next Hop is given by the following rule:

- $N = D$ for ZigBee end devices where $D > A + Rm \cdot Cskip(d)$
- $N = A + 1 + \left\lfloor \dfrac{D - (A+1)}{Cskip(d)} \right\rfloor \times Cskip(d)$, otherwise

If the expression is false, then the destination is not a descendant and the message should be routed through A's parent.

III. RESULTS AND DISCUSSION

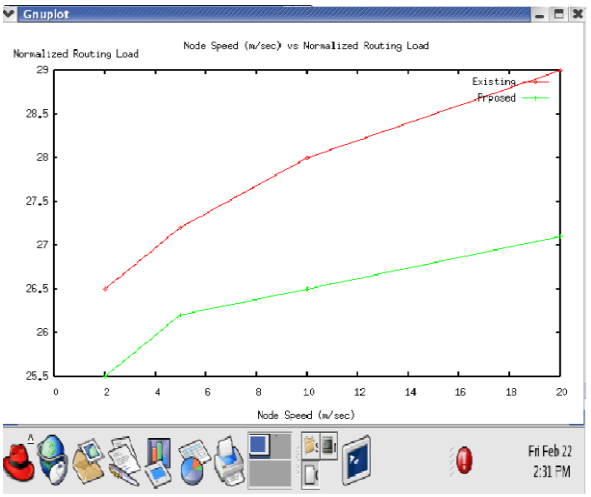

Figure.2. Node Speed (m/sec) vs Normalized Routing Load

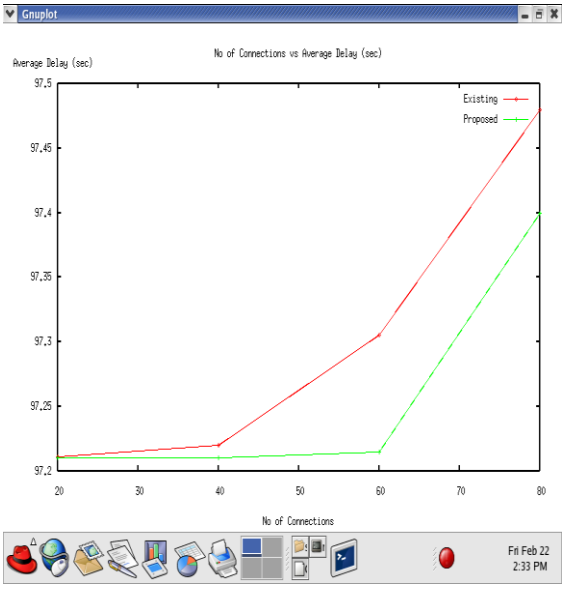

Figure.3. No of Connections vs Average Delay (Sec)

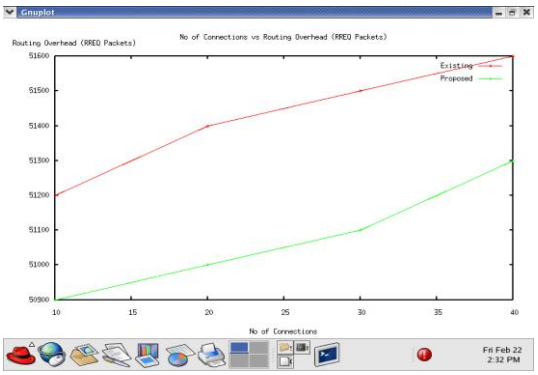

Figure.4. No of Connections vs Routing Overhead (RREQ Packets)

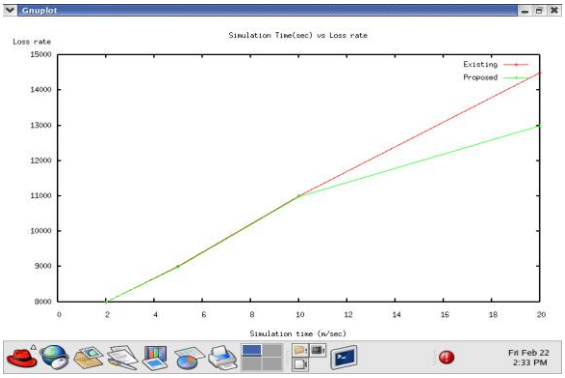

Figure.5. Simulation Time vs Loss Rate

IV. CONCLUSION

SCADA systems are not designed with security in mind rather the priority for developers has been reliability, availability, and speed. It does not mean the system cannot be secured. If we can analyze a particular system's performance, functions, features and capabilities, we can address its limitations. A generic framework for SCADA provides a tool to understand the system's capabilities, and how the components in the system relate and interface with each other. With that information about the system, we can begin the process of securing it. The proposed framework provides realistic evaluations of SCADA systems by adding real devices into the simulation. Two practical case studies on smart grid simulation were conducted with DDoS and spoofing attacks being presented. Results demonstrate that SCADASim closely simulates the realistic behaviour of actual SCADA devices. In Future we are going to enhance this by implementing cross layer mitigation technique.

REFERENCES

i. *Abdun Mahmood, and Zahir Tari, Carlos Queiroz, "SCADASim- A Framework for Building SCADA Simulations" IEEE transactions on smart grid, vol.2, no.4 dec 2011.*

ii. *C. Beaver, D. Gallup, W. Neumann, and M. Torgerson, Key Management for SCADA 2002. [Online]. Available:http://www.sandia.org/scada/documents/013252.pdf*

iii. *K. P. Birman, J. Chen, K. M. Hopkinson, R. J. Thomas, J. S. Thorp, R. Van Renesse, and W. Vogels, "Overcoming communications challenges in software for monitoring and controlling power systems," Proc. IEEE, vol. 93, no. 5, pp. 1028–1041, May 2005.*

iv. *D. Choi, H. Kim, D. Won, and S. Kim, "Advanced key management architecture for secure SCADA communications," IEEE Trans. Power Del., vol. 24, no. 3, pp. 1154–1163, Jul. 2009.*

v. *G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski, "Collaborative, trust based security mechanisms for a regional utility intranet," IEEE Trans. Power Syst., vol. 23, no. 3, pp. 831–844, Aug. 2008.*

vi. *R. D. Colin, C. Boyd, J. Manuel, and G. Nieto, "KMA—A key management architecture for SCADA systems," in Proc. 4th Australasian Inf. Security Workshop, 2006, vol. 54, pp. 138–192.*

Efficient Secure Group Communications for SCADA Donghyun Choi, Student Member, IEEE, Sungjin Lee, Dongho Won, and Seungjoo Kim, Member, IEEE.IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 25, NO. 2, APRIL 2010.

vii. *N. Falliere, L. O. Murchu, and E. Chien, W32.Stuxnet Dossier, Symantec Tech. Rep. 1.4, 2011.*

viii. *R. Graham and D. Maynor, "SCADA security and terrorism: We're not crying wolf," presented at the Black Hat Federal, Washington, DC, 2006.*

V.M.Igure, S.A.Laughter, and R.D.Williams, "Security issues in SCADA networks," in Comput. Security, Mar 2006, vol. 25, pp.498–506.

AUTHOR'S PROFILE

First author- S.Thamaraichelvi. She received her B.E. degree in Electrical and Electronics engineering from the reputed college of Anna University, India in 2011. She is pursuing her M.E in Applied Electronics from Sasurie College of Engineering-Affiliated to Anna University, Tamil Nadu, INDIA. Her research interest in Network Security.

Second author- N.Rajesh Kumar. He received his B.E. degree in Electronics and Communication engineering from the reputed college of Anna University, India. He received his M.E in Computer and Communication Engineering from the reputed college of Anna University, Tamil Nadu, INDIA. He is doing his research in optimized security challenges in scada systems environment. Presently he is working as Assistant Professor in sasurie college of engineering, Tirupur.

Third author- B.Dineshshankar. He received his B.E. degree in Electronics and Communication engineering from reputed college of Anna University, India. He is pursuing his M.E in Applied Electronics from Sasurie College of Engineering-Affiliated to Anna University, Tamil Nadu, INDIA.