Securing Gateways within Clustered Power Centric Network of Nodes

QAISAR JAVAID*, MUHAMMAD DAUD AWAN*, AND SYED HUSNAIN A NAQVI*

RECEIVED ON 19.01.2015 ACCEPTED ON 28.05.2015

ABSTRACT

Knowledge Networks are gaining momentum within cyber world. Knowledge leads to innovation and for this reason organizations focus on research and information gathering in order to gain and improve existing knowledge. This of information era, which is primarily based on world wide web technologies, enables significantly expanded networks of people to communicate and collaborate 'virtually' across teams, across entire organizations and across the world, anytime and anywhere. Innovations in computing and telecommunications have transformed the corporations from structured and manageable types to interwoven network of blurred boundaries such as; ad hoc networks and mobile wireless networks, etc. This study explores knowledge networks in Information Technology and security leaks that are found, as well as measures that are taken to counter this menace which is coming up with optimal Secure Clustered Power Centric node network. The paper concludes these measures, evaluating and integrating them to come up with a secured network design.

Key Words: Cyber Technology, Knowledge Networks, Power Centric Nodes, Security, SCADA.

1. INTRODUCTION

Virtual Knowledge Networks are proficient enough to form interactive learning mechanism, promoting innovation and bringing new advantages with it. Cyber Knowledge Networks consist of different mediums; social networking (blogs, twitter, etc.) and mobile networks (such as smart phones) that convert the collected information into semantic networks through interlinking agents [1]. These networks are highly complex networks in terms of transportation of data and mobility [2].

A network composes of connecting different nodes or vertices that are correlated to each other with the Internet being combination of millions, or even billions of these vertices. An analyst might have asked the question [3], which node would prove most critical to the connectivity of network if it has been removed? But this question is not much useful in a huge network - as single node will not have much effect when detached and it is impractical to portray a meaningful picture from all these vertices. Thus analysts try to convert these connections to statistical data that would tell the path lengths and degree of distributions which helps in measuring network structure, properties and behavior. The aim to create a network model is to understand its structure and how they would interact

* Faculty of Computer Science, Perston University, Islamabad.

in such a huge network. Then it determines the behavior of this network, for example, how the network structures would affect the traffic on the Internet.

This research would further highlight the various types of knowledge networks that are working with different levels of security safety measures to protect the information being transmitted within these networks. The security mechanisms being implemented would be validated by mapping onto the cyber security standards.

Designing an optimum secured network design and implementing security in knowledge networks is very crucial for future developments. Creating intelligent clusters makes the knowledge networks easy to manage and monitor for faults and intrusive malicious activities that endanger this massive network. And, IPSec protocol has been 70% implemented as it is standardized by IETF (Internet Engineering Task Force). Security within knowledge networks would add value to knowledge management and business intelligence techniques for further improvements and enhancement. Consumers of knowledge networks need to be assured of secure transmission and storing of their highly valuable data.

2. RELATED WORK

While studying the behavior of knowledge networks such as ad hoc mobile and wireless sensor, there are several associated vulnerabilities and threats that keep the secure transmission of endanger. And to encounter these threats different security measures are implemented. One of such architectures proposed [4] is RON (Resilient Overlay Network). It provides distributed Internet Applications with an architecture that would detect and recover, within several seconds, from path outages and periods of degraded performance. Freenet [5] is another example of peer-to-peer network application which permits publication, retrieval and replication of data keeping anonymity of both the authors and readers. Files are referred in such location transparency manners, dynamically allocate storage resources near to the requestor and delete it later. Likewise, many such developments are in the pipeline that would be discussed in this study.

With the emergence of wireless communications, low cost sensor networks are developed that are composed of different sensor nodes, densely placed in their positions that are not predetermined. Sensor network has an onboard processor which computes raw data and transmits only the required partially processed data [6]. Whereas in ad-hoc networks throughput is increased by using techniques such as Watchdog and Pathrater that identify misbehaving nodes and helps routing protocols to avoid these nodes respectively [6]. Afterward, a novel GPSR (Greedy Perimeter Stateless Routing) protocol [7] for wireless datagram networks which use the positions of routers and a packet's destination to make decisions for packet forwarding. It is a greedy approach to transmit information knowing only about the immediate neighbors of the routers. By maintaining the state only about the local topology, GPSR scales are better than ad-hoc and are the shortest path algorithms in per-router state as the number of network destination increases. Hence, foremost dominant factors considered in scaling of routing protocol are the number of routers in a domain and the frequency with which a topology changes.

Tasks such as authentication, data integrity, intrusion detection and prevention, firewall systems; and threats recognized such as; routing attacks, man-in-the-middle, and privacy; are all concerns of security within the cyber knowledge world. As the networks are growing, fast and advancing by incorporating cloud computing, the mobile internet, VOIP (Voice Over Internet Protocol), intelligent systems, smart phones as well as home environments,

compel the security to be more complex as the number of countless attacks increases from malicious users. Researchers [8] finds the need of security measures as strong as the attackers and intruders to these systems; therefore delivering the internet world with the novel algorithms, frameworks, and theories, that improve the ever increasing threat to Internet security and leverages. The work also recognizes the recent security measures and proposed architectures, topology parameters and operations, reactive and reconfiguring mechanisms, and human advisory.

Furthermore, research highlights the various types of knowledge networks that are working with different levels of security precautions protecting the information being transmitted within these networks.

2.1 Group Authentication

Commonly, there are two types of authentications; knowledge based (e.g. passwords) and key based authentication (e.g. public/private key encryption). Knowledge based authentication has some flaws, the main being that passwords could be hacked, likewise key based authentication has concerns with the computational time involved using large integers. Research [9] analyzed the strengths and weaknesses of several protocols that form a secure network using the experimental channel. Furthermore, extended protocols proposed two group protocols that works in different levels of trustworthiness and resist combinatorial attack with additional feature being less hungry in computing power. A new concept of a local PKI has been introduced, which binds information such as identities, public keys, and context collectively in an authenticated way.

2.2 BOTNET Boost-up Detection System

Botnet provides a platform for serious threats encounters which include distributed denial of service, information stealing and spamming. As the networks are growing and high scalability is required by Botnet detection systems, the study [10] presents three unique contributions towards enhancing the functionality of current detection system. Firstly, they built a novel system to detect drive-by downloads, which serve as the primary way for Botnet infection. Furthermore, they proposed a new P2P C&C Botnet detection system structures adopted to identify attacks that could be disrupted the network. Finally, a framework is provided for traffic analysis to boost the effectiveness of present Botnet detection system. Thus, sending the network traffic associated with these hosts to boost-up existing detection systems include the algorithms for novel Botnet-aware and adaptive packet sampling with scalable flow-correlation technique.

2.3 Multistage Attack Recognition System

Malicious attacks by hackers and intruders exploit vulnerabilities in deployed systems through several sophisticated techniques that cannot be prevented by conventional measures, such as user authentication, firewalls and access controls. Therefore, automated detection and prevention systems are needed to detect abnormal events by monitoring network system events and traffic [11]. NIDS (Network Intrusion Detection Systems) and NIPS (Network Intrusion Prevention Systems) are technologies that look over the network traffic and analyze system behavior to provide better protection against attacks. The existing implementation of IDS lack the scalability to support the emergence of new protocols, as well as a gigantic increase in network speed, and services. The research [11] focused on two different problems for the NIDS: missing alerts due to packet loss as a result of NIDS performance limitations; and the huge volumes of generated alerts by the NIDS makes event observation tedious. And proposed methodology for analyzing alerts correlation has been

presented to provide the security operator with a global view of the security perspective. Missed alerts are recovered using a contextual technique to detect any-multi-stage attack set-up. These algorithms have been implemented in a tool called MARS (Multi-stage Attack Recognition System) consisting of a collection of integrated components.

2.4 Centralized Host-Based Security Scanning Architecture

Security threats and contravention in an organization's network infrastructure can cause critical interruption of business progression and lead to information and investment losses. A strong security system is essential for vulnerability assessment and enterprise. The traditional host based vulnerability and security analysis technique, though effective for individual systems does not keep up with the trend of knowledge sharing and global perspective. The centralized architecture [12] reduces the issue of knowledge duplication and eliminates the need to recurrently update the client because of its separation of analysis from the data collection part. Furthermore, it performs all the analysis activity and report generates on the centralized server.

2.5 Security of Cluster-Based Communication Protocols

Ad hoc networks and WSN (Wireless Sensor Networks) are comprised generally of tiny sensor nodes with limited resources, and are swiftly emerging as a technology for low cost, large scale, automated sensing and monitoring of different environments of interest. Cluster based communication has been proposed for these networks for various reasons such as scalability and energy efficiency. Study focused on adding security to cluster-based communication protocols in homogeneous WSNs with resource constrained sensor nodes and a security solution for LEACH, a protocol where clusters are created periodically and dynamically [13].

SLEACH is a modified form of LEACH with cryptographic protection against outsider attacks. It precludes an intruder from becoming a CH (Cluster Head) or injecting false sensor data into the network. SLEACH is quite efficient, and preserves the structure of the original LEACH, including its ability to carry out data fusion.

2.6 Turing Assessor

Creating security metrics is a challenging task as the network communicates with an external environment which makes it very vulnerable to active and passive threats i.e. eavesdropping, updating, modifying or deleting packets over the communication channel. This research [14] has proposed a new theory to evaluate security properties in system level by applying the standard reduction technique. A security measure metric Turing Assessor [14] evaluated for a decomposed network for security qualification, resultantly, found a complete network that is robust in model.

2.7 Supervisory Contro and Data Acquisition Systems - A Test Bed

Sridharan [15] addressed the vulnerabilities assessment in Smart Grid concept in which he categorized the devices in term of risk and associated threat and vulnerabilities. Research focused on four cases in which an attack can be carried out on the devices which are, attack on the computer accessing the SCADA system, insider attacks, attack on the SCADA network, and direct manipulation or reprogramming of the device. A network monitoring model [15] has been projected with the state estimation theory, and network investigations to identify and articulate any malicious attacks on the SCADA network.

3. PROBLEM FORMULATION

Knowledge networks as complex as it is harder to secure against intruding parties that can be malicious users, hackers, crackers, unauthorized access, etc., spreading destructive viruses and Trojans, making dissemination of important information a risky endeavor. However, there have been considerable researches done to embed security in knowledge networks that are often termed as sensor networks, such as MANET (Mobile Ad-hoc Networks), wireless networks, semantic web, etc. Still there are gaps left to be taken care of.

3.1 Back Track Software

Several software are available that help the intruder to hack the systems over the open networks whether it is an enterprise or a home based network. Back track [16] application have been distributed by Linux as a penetration testing tool that is used for security tests of LANs, Wi-Fi, Bluetooth and so on. On the other hand, skilled hackers use this same application to get automated access to the open network.

3.2 Massive Knowledge Network

The network channels are used for different forms of communication which are required to be safe from eavesdropping. So far, it is an extremely demanding task with huge complexity to counter attack an intruder whose origin and even the way of attack was hard to be identified in the massive network. And to come up with a well formed strategy a controlled analysis is required so that risks could be identified.

3.3 Research Problem

The research questions or concerns posed by the research at hand are:

(i) Determining the optimum solution to knowledge networks security, integrating the security measures formed until now.

(ii) To come up with the best network design that enables the solution to work securely.

(iii) How to keep the sender hosts, receiver hosts and communication channel be secure from network attacks?

(iv) What mechanism is adopted to monitor such a huge network?

(v) What would be the optimum security standards that are to be followed?

4. PROPOSED SOLUTION

The security concerns in knowledge networks would have to be tackled by adopting various means that would comprise of secure communication protocols and cryptographic algorithms. These mechanisms would enforce security parameters [17]:

Confidentiality: Data transmitted between two endpoints remains private.

Integrity: The data does not get tampered with during transmission.

Availability: The endpoints are accessible whenever required.

Authenticity: Data sender has to authenticate himself and data receiver should not be spoofed.

IETF has greatly contributed in standardizing different protocols for providing open network security. At the network layer of TCP/IP communication protocol model, IPSec (Internet Protocol Security) is implemented to keep the data exchange secure at different configuration parameters such as; (i) gateway-to-gateway, (ii) gateway-to-host, and (iii) and host-to-host communication [17]. IPSec is known for providing confidentiality, data-origin

authentication, integrity and prevention against replay attacks by using security protocols; AH (Authentication Header), and ESP (Encapsulated Security Payload) in combination with IKE (Internet Key Exchange).

This research focuses on forming a clustered network combining towns and cities and thus, catering to a massive network of nodes. And, the routers are the nodes that would be power centric and behave intelligently. Thus, IPSec is configured on routers to implement gateway-to-gateway security as node-to-node security becomes too annoying.

5. OPTMIAL SECURED NETWORK DESIGN

5.1 Cluster of Nodes

his research study proposes a security mechanism forming a network design in a clustered manner. Based on literature review, it is learnt that there have been many mechanisms already proposed. This study gathers the most appropriate features of these and incorporates them into a clustered network that enables monitoring in a dense network of nodes. Then:

(i) The Best and most appropriate security mechanisms are filtered through literature review and refined to integrate within the clustered network.

(ii) The knowledge networks are broken into dense clusters given some threshold parameters (e.g. area of each cluster).

(iii) The routers in these clusters are made intelligent being power centric with the ability to diagnose sender and receiver hosts for any type of malicious activities.

5.2 Power Centric Nodes

Systems running on a power supply are also known to be threatening to knowledge networks in term of sharing informative data along the network channel. In this research its already clarifies in Sridharan's [15] proposed test bed – SCADA, that monitors the cyber security in a multi-laboratory configured in Georgia. Routers in a clustered network termed as central nodes or cluster head in this research study, hold such monitoring system and act as power centric for the traffic coming from different gateways.

Security in power systems themselves would not be ignored as well when creating a robust network [18]. As there are several mechanisms formed for the security of NCS (Network Controlled Systems), such optimal solution is designed to protect routers and gateways, sensing the malicious data corruption and attacks in information channels connecting routers and within the routers itself. Then there is centralized host-based security scanning architecture [12] that is also a part of the routers within a cluster.

5.3 Monitoring for Intrusive Activities

Boost-up Botnet detection system [10] is there contributing three novel strategies for tackling the cyber-attacks as illustrated in section 2.3, these contributions boost the effectiveness and scalability of existing Botnet detection systems. Algorithms for adaptive packet sampling and novel Botnet aware system are there with scalable flow-correlation technique and are purposed for this research model. Network intrusion detection and prevention systems are inbuilt in central network connecting devices such as routers (nodes) integrating them with the tool called MARS (Multistage Attack Recognition System) [11] which includes a collection of integrated components such as: alert correlation, graph reduction, and alert aggregation.

5.4 IPSEC Network Protocol

IPSec is a standard security protocol [19] that 'encapsulates' an encrypted network layer packet inside a standard network packet keeping the encryption transparent to intermediate nodes that must process packet headers for routing, etc. authentication, encryption, encapsulation, which is done on outgoing packets being sent to the network. And, thus incoming packets are decrypted, de-capsulated and verified upon receipt. Key management in this system is simpler.

5.5 HADM-KRS

The latest versions of HADM-KRS (High Availability of Decentralized Cryptographic Multi-Agent Key Recovery System) [20] are employed, that is complying with the NIST framework for the latest key recovery system. Additionally, the system administrator allows specifying the minimum number of KRAs (Key Recovery Agents) as per security policies and requirements meeting all the legality concerns. These versions provide the security platform with enhanced performance, robust and fault tolerant network in terms of secrecy and availability.

5.6 Secure Routing in Cluster based WSNs using Symmetric Cryptography with Session Keys

Sensors which are acquiring huge attacks are not suitable for complex cryptographic algorithms due to its low computational power and limited resources. An implemented symmetric key algorithm with session keys carry better security as compared to previous secure routing algorithm in cluster wireless sensor networks [21].

5.7 Verification of Network Model

A simulation [22] for producing real-time network traffic is adopted that generated test data and cyber-attacks in the presence of security intrusion detection systems. The security protocol being used is IPSec on each router in the networks. A network design (Fig. 1) is thus proposed to hold power centric intelligent nodes (routers) within clustered knowledge networks. In a real network system, the clusters would be formed such that each town or city would have one intelligent cluster.

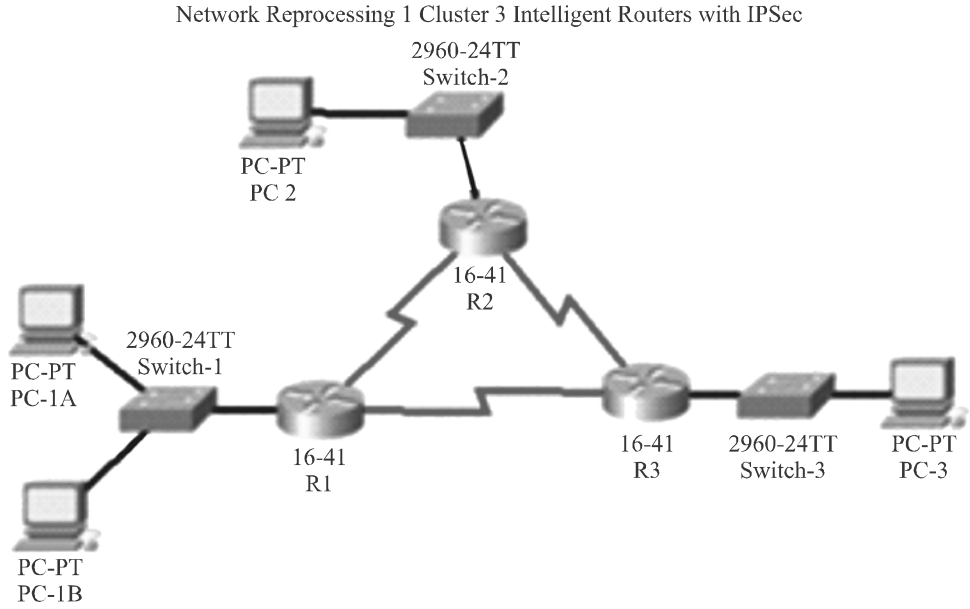

FIG. 1. A CLUSTERED NETWORK DESIGN HAVING 3 INTELLIGENT ROUTERS

5.7.1 Logical Verification of Design

Proposed network designed involves the conditional implementation of statements that specify the attribute or determine its value. The basic feature includes Parent-child connection, subnet implementation, services stored on device and access rights list.

5.7.2 Visually Verified Features

The visual shell of the modeling process to verify the design features includes the graphical representation of design model and the attribute values. The design model features that have been verified visually are Graphic connections, IP addressing, and Network model saving process.

5.8 Comparison of S-LEACH and SRCWSNS

SLEACH is one of the well-known protocols used in cluster based MANETs and WSNs. SLEACH mitigates almost all attacks excluding 'sink hole' and 'wormhole' attacks. The main aim of sinkhole attack is to steal the information which will lead to wormhole attack (Fig. 2).

Consider the following scenario will give explanation for the mitigation of sinkhole attack. Here node M act as the

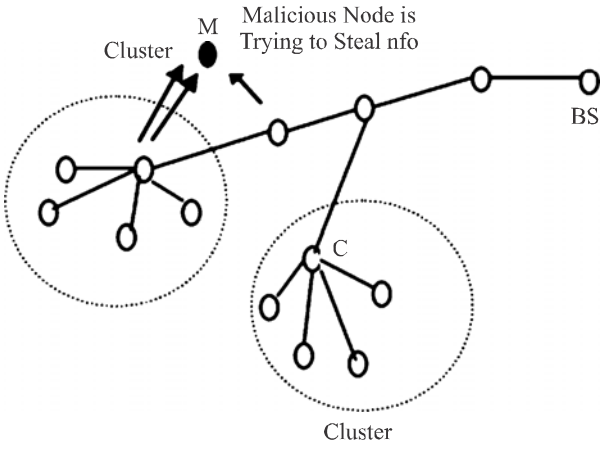

FIG. 2. MITIGATION OF SINKHOLE ATTACK [21]

valid node, which compromises the location of neighbors cluster head node. The forwarding cluster head checks the identity of M node and checks the symmetric key. Even if M got the symmetric security key the forwarding cluster head checks loading time of the node or bootstrap time, it ensures more security. These keys are encrypted by using 'blowfish symmetric algorithm', so to find out where these keys are very difficult. It takes more time to crack the keys, and in the meanwhile the base station will change the session key. So to steal the information from nodes, the intruder again tries to decode the content to get the session key.

Even if the malicious node will compromise on one node there is no risk to compromise other nodes through this one. So the effect of node compromising will be controlled to only that specific part of the network. Similarly the forwarding node will find out the malicious node and also mitigates a wormhole attack.

6. CONCLUSIONS

An accurate and detailed IDS and IPS are strongly desired to be implemented in the cyber security area.

The functionality of network design and attacks verified and validated through some of different modeling techniques. SCADA monitoring system deployed on central nodes in a clustered network, act as power centric for the traffic coming in from different gateways integrating with the tool MARS that include components of alert correlation, graph reduction, and alert aggregation.

Standard Network layer IPSec security protocol secure the centric node and cluster network communication, as it provided the security scheme of confidentiality, origin authentication, integrity and prevention against replay attacks in addition to error detection and diagnostic capability. Whenever, communication data packets are about to depart a cluster network centric node and when

getting to a destination node, security policies are enforced on endpoints, routers, gateways, firewalls.

In response to the Problem statement, Clustered network design having power centric node successfully securing the gateway by implementation of the studies and illustrated standards, algorithms, techniques.

ACKNOWLEDGEMENTS

Author would here like to express his gratitude to the people who have been very helpful to him during the time it took me to write this paper. First and foremost authors that author would like to thank his supervisors, referees and reviewers for their valuable feedback on earlier drafts which have been improved this paper.

REFERENCES

[1] Reddy, R., "Personal Knowledge Networks in the Mobile Millennium", Proceedings of IEEE International Symposium on IT in Medicine and Education, West Virginia University, USA, 2009.

[2] Nousala, S., "Understanding the Value and Transference of Tacit Knowledge in Socio-Technical Networks and Complex Systems: Study of Simultaneous Internal and External Organizational Knowledge Networks", Proceedings of 8th International Conference on ITST, RMIT, Australia, 2008.

[3] Newman, M., "The Structure and Function of Complex Networks", University of Michigan, USA, 2003.

[4] Andersen, D., Balakrishnan, H., Kaashoek, F., and Morris, R., "Resilient Overlay Networks", Proceedings of 18th ACM Symposium on Operating Systems Principles), Banff, Canada, October 2001.

[5] Clarke, I., Sandberg, O., Wiley, B., and Hong, T., "Freenet: A Distributed Anonymous Information Storage and Retrieval System", National Science Foundation and Marshall Aid Commemoration Commission, 2001.

[6] Akyildiz, I., Su, W., Sankarasubramaniam, Y., and Cayirci, E., "A Survey on Sensor Networks", IEEE Communications Magazine, Volume 40, No. 8, pp. 102-114, 2002.

[7] Karp, B., and Kung, H., "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", MobiCom, Harvard University, 2000.

[8] Thames, J., "Advancing Cyber Security with a Semantic Path Merger Packet Classification Algorithm", Ph.D. Thesis, Georgia Institute of Technology, 2012

[9] Harn, L., and Lin, C., "An Efficient Group Authentication for Group Communications", International Journal of Network Security& Its Applications, Volume 5, No. 3, May, 2013.

[10] Zhang, J., "Effective and Scalable Botnet Detection in Network Traffic", Ph.D. Thesis, Georgia Institute of Technology, 2012.

[11] Alserhani, F., "A Framework for Correlation and Aggregation of Security Alerts in Communication Networks", Ph.D. Thesis, University of Bradford, 2011.

[12] Rakshit, A., "A Host-Based Security Assessment Architecture for Effective Leveraging of Shared Knowledge", Masters Thesis, Kansas State University, India, 2009.

[13] Ferreira, A., Vilaca, M., Oliveira, L., Habib, E., Wong, H., and Loureiro, A., "On the Security of Cluster-Based Communication Protocols for Wireless Sensor Networks", Federal University of Minas Gerais, Brazil, 2005.

[14] Zhu, H., Chigan, C., and Bao, F., "Turing Assessor: A New Tool for Cyber Security Quantification", Proceedings of IEEE WCNC, 2006.

[15] Sridharan, V., "Cyber Security in Power Systems", Masters Thesis, Georgia Institute of Technology, 2012.

[16] Backtrack-linux.org, www.backtrack-linux.org, © Backtrack Linux 2014.

[17] Cirani, S., Ferrari, G., and Veltri, L., "Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview", Algorithms, Volume 6, pp. 197-226, 2013.

[18] Teixeira, A., "Toward Secure and Reliable Networked Control Systems", Masters Thesis, KTH Royal Institute of Technology, 2011.

[19] Blaze, M., Ioannidis, J., and Keromytis, A., "Trust Management and Network Layer Security Protocols", AT&T Laboratories, Distributed Systems Labs, University of Pennsylvania, 2000

[20] Kanyamee, K., and Sathitwiriyawong, C., "High-Availability Decentralized Cryptographic Multi-Agent Key Recovery",The International Arab Journal of Information Technology, Volume 11, No. 1, January, 2014.

[21] Rao, R, "Secure Routing in Cluster based Wireless Sensor Networks using Symmetric Cryptography with Session Keys", International Journal of Computer Applications, Volume 55, October 2012

[22] Costantini, K.C., "Development of a Cyber Attack Simulator for Network Modeling and Cyber Security Analysis", Masters Thesis, Rochester Institute of Technology, 2007.