International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

CLUSTER BASE KNOWLEDGE NETWORKS SECURITY AND OPTIMIZATION USING A BEE-INSPIRED IROUTCLUSTER PROTOCOL

Qaisar Javaid1,2, Dr. Muhammad Daud Awan1, Dr. Syed Husnain A Naqvi2
1Faculty of Computer Science, Preston University Islamabad, Pakistan
2International Islamic University Islamabad, Pakistan

Abstract

Knowledge Networks are gaining momentum in cyber world. Knowledge leads to innovation and for this reason organizations try to capture knowledge both circulating inwards and outwards. In this age of information era based on technology, knowledge and informational processes are privileged outcomes. Wonderful innovations in computing and telecommunications have transformed organizational forms to include new networks. These networks could be individual and cognitive, distributed work group networks, as internal organizational networks (Intranets), and as external network connections via Extranets. Organizations have changed from structured and manageable type to interwoven network of blurred boundaries such as; ad hoc networks and mobile wireless networks, etc. Knowledge is shared through social interaction in informal networks in an organization that has now shifted towards Cyber Technology. This study explores the means of knowledge networks in Information Technology and simulated results to reach an optimal cluster size of nodes in knowledge networks that would ensure the security towards leaks that are found in a massive network and measures taken to counter this menace. The paper concludes these measures, experimenting and evaluating the results to come up with an optimal solution.

Index Terms — Clustered Network, Cyber Technology; Knowledge Networks; Power Centric Nodes; iRoutCluster Protocol, Security; SCADA.

Introduction

This Network is made up of connecting different nodes or vertices that are correlated to each other. Internet or World Wide Web is combination of millions even billions of vertices. Virtual Knowledge Networks are good to form interactive learning mechanism, promoting innovation and bringing new advantages with it. Virtual or Cyber Knowledge Networks consist of different mediums; social networking (blogs, twitter, etc.), mobile networks (such as iPhone) that converts the collected information to semantic network through interlinking agents [14]. Knowledge networks are highly complex networks in terms of transportation of data and mobility [15]. There are various questions that arise [16], like an analyst can ask: which node would prove most crucial to network connectivity if it is removed? This probability would be minimal when talking about such a large network. To draw a meaningful picture and form an understanding from all these vertices is unbelievable. Thus analysts try to convert these connections to statistical data that would tell path lengths and degree distributions to help in measuring network properties and structure. Network models are created to understand structure and how the interactions are made in such a huge network. Then it determines the behavior of this network, for example, how the network structure would affect the traffic on the Internet. In the seven layers OSI model the third layer is network layer that is responsible for packet forwarding including routing through intermediate routers.

Finding an optimum solution to implementing security in knowledge networks is very crucial for future developments. Any future developments towards knowledge networks would require a strong foundation that could not be outperformed by security threats. It would be thoroughly tested against current penetration techniques employed by intruders. 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.

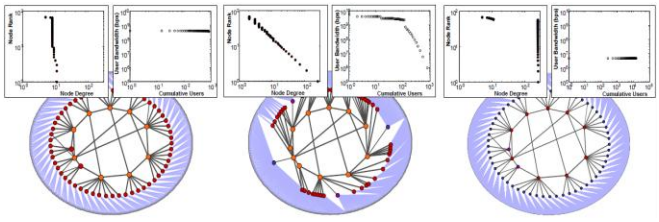
Background and Related Work

When studying the behavior of the networks, there are threats of security breaches that endanger the secure transmission of information. Topology of the Internet has to be first understood to address the criticalities of this complex infrastructure. First-principles theory [17] reflects the constraints and tradeoffs in network topology. It claim very simple models that links bandwidth and connectivity into the hard technological constraints jointly with abstract models defining user demand and network performance. Cisco 12416 Gigabit switch router (GSR) is limited by its bandwidth and number of available line-card connections it has

ISSN:2319-7900

i.e. 15 for which it is configured and throughput per degree is constrained by line-card maximum speed of 10 Gbps. Total bandwidth increases as the number of connections increase but when the connections exceed 15 it starts to degrade. There can be maximum possible connections up to 120 for this router but connections exceeding 15 are not recommended. There are different types of bandwidths requests as per user ranging from 56 Kbps to very low number of users requesting 10 Gbps. Thus, considering these requirements the network has to be designed and build. For the network solution providers the economic constraints also pose the limitations of the type of network deployment. They are influenced by the number of users on the network and their increasing bandwidth requests with time.

In Figure 1, where the network core supports different types of variability in end user bandwidths at the edge. The network in Figure 1(a) provides high bandwidth to end users; the network in Figure 1(b) supports end user bandwidth require that are highly variable; and the network in Figure 1(c) provides uniformly low bandwidth to end users. Hence, from an engineering standpoint, not necessarily any implied relationship between a network degree distribution and its core structure, there is also no implied relationship between a network's core structure and its overall degree distribution [17].



(a) (b) (c)

Figure 1. Distribution of Node Degree in Different Topologies with Different Bandwidths.
(a) A Uniformly High Bandwidth End-Users
(b) Highly Variable Bandwidth
(c) Uniformly Low Bandwidth [17]

Topology Metric

Identifying that the primary purpose for building a network is to carry effectively a projected overall traffic requirements, we consider several means for evaluating the performance of the network. The metrics to understanding and evaluating network topologies have been dominated by graph-theoretic quantities and their statistical properties, e.g., node-degree distribution, expansion, resilience, distortion and hierarchy are commonly used metrics [29].

Performance Related Metric

Network performance is as the maximum *throughput* on the network under heavy traffic conditions based on a gravity model as in Equation (1) [30]. That is, considering the flows on all source destination pairs of edge routers, such that the amount of flow X_{ij} between source i and destination j is proportional to the product of the traffic demand x_i, x_j at end points i, j, $X_{ij} = {}_{\alpha xixj}$, where α is some constant. We compute the maximum throughput on the network under the router degree bandwidth constraint.

$$\max_{\alpha} \quad \sum_{ij} \alpha x_i x_j \qquad (1)$$
$$\text{s.t} \quad RX \leq B,$$

Where X is a vector obtained by stacking all the flows $X_{ij} = \alpha x_i x_j$ and R is the routing matrix (defined such that $R_{kl} = \{0,1\}$ depending on whether or not flow l passes through router k). We use shortest path routing to get the routing matrix, and define B as the vector consisting of all router bandwidths according to the degree bandwidth constrain.

In computing the maximum throughput of the network, obtained the total traffic flow through each router, which terms as *router utilization*. Since routers are constrained by the feasible region for bandwidth and degree, the topology of the network and the set of maximum flows will uniquely locate each router within the feasible region[17].

Counter Measures on Security Threat

Before the proposed theory there have been numerous measures proposed to counter these threats different security measures were implemented. One such architecture proposed [18] was Resilient Overlay Network (RON). It provided distributed Internet Applications with an architecture that would detect and recover, within several seconds, from path outages and periods of degraded performance. RON is an overlay of application layer on top of Internet routing substrate that monitors the quality of functioning of Internet paths amongst them. This information is used further to decide packets to route straight over the Internet or through the RON nodes using optimum application specific routing metrics.

Feature of Wireless Ad-hoc and Sensor Network.

With the emergence of wireless communications low cost sensor networks are developed. The sensor networks are composed of different sensor nodes which are densely placed as their positions are not predetermined. Sensor network has an onboard processor that processes and computes raw data and transmits only the required and partially processed data [19]. Such sensor applications are deployed in healthcare, military, and homes. Characteristics like self-organization, fault tolerance, and rapid deployment make it

ISSN:2319-7900

useful to the military in tasks like command, control, surveillance, communication, targeting, etc. Such applications need to employ characteristics of wireless ad hoc networking techniques. There are lots of differences in traditional wireless ad-hoc networks and sensor networks and researchers want to diminish these differences and are trying to cater these loop holes. In ad-hoc networks throughput is increased by using techniques like *watchdog* and *pathrater* that identifies misbehaving nodes and helps routing protocols to avoid these nodes respectively [20]. Then there is GPSR-Greedy Perimeter Stateless Routing protocol [21] for wireless datagram networks that use 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. GPSR scales better than ad-hoc and shortest path algorithms as the number of network destination increases keeping in per-router state in a local topology.

Peer-to-peer network

Freenet[22] is another example of peer-to-peer network application. It permits retrieval, publication, and replication of data keeping anonymity of both authors and readers and taking measures to enhance the security of information storage. Freenet operates as a network of similar nodes that make a pool of storage space to store data and collaboratively rout requests for data to its most likely physical place. Similar to distributed hash tables, Freenet protocol uses a *key-based routing* protocol. There is no centralized location or broadcast search to locate data. It is designed keep protecting the anonymity of readers and authors and data is stored and routed dynamically at location independent distributed file system pooled by the nodes.

Likewise, many such developments are in the pipeline that would be discussed in this study. This research would further highlight the various types of knowledge networks that are working with different levels of security precautions protecting the information being transmitted within these networks.

Evaluating Problem Domain

Knowledge Networks as complex as it is, 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. There have been considerable researches done to embed security in knowledge networks that are often termed as sensor networks, mobile ad-hoc networks (MANET), wireless networks, semantic web, etc. Still there are gaps left to be taken care of.

Back Track Software

There is software available that helps the intruder to hack the systems over the open networks whether it is an enterprise or a home based network. Back track [23] application has been distributed by Linux as a penetration testing tool that is used for security tests of LANs, Wi-Fi, Bluetooth and the list goes on. The same application is also the favorite of skilled hackers who get automated access to the open network.

Massive Knowledge Network

The network channels are used for different forms of communication that are required to be safe from eavesdropping. The high magnitude of nodes present in knowledge networks is itself a problem. It is hard to manage and monitor for external threats that are vast in number and type.

Research Problem

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

1. *Determining the optimum solution to knowledge networks security, integrating the security measures formed till now;*
2. *To come up with the best network design that enables the solution to work securely;*
3. *How can the sender and receiver hosts and communication channel between them be isolated from network attacks?*
4. *What mechanism is adopted to monitor such a huge network?*
5. *What would be the optimum security standards followed? and*
6. *How these cyber security standards are implemented?*

Authenticating the parties on both ends in knowledge networks, then the data being transmitted needs to be safely reach on to the other end without being hijacked in the middle, intrusive behavior within the networks has to be discouraged through early detection and prevention mechanisms and implementing firewalls are all tasks to be considered in this research for implementing optimal security in cyber networks. There are different types of routing attacks, man-in-the-middle, and lack of privacy concerns. As the networks have advanced considerably including cloud computing, the mobile internet, voice over IP (VoIP), intelligent systems, smart phones as well as home environments give way to countless attacks from malicious users. Intermittently connected networks thus also have problem of not having a connected path between desired nodes where communication is required [1]. PROPHET [1] is proposed which enables the network to deliver more messages than other routing

ISSN:2319-7900

protocols like epidemic routing with lower communication overhead. PROPHET being a probabilistic routing protocol learns the predictable communication channels between the parties as real users do not move randomly but in some predictable fashion. Repeatedly followed communication channel is observed and it is inferred that the connection would be used in future too.

Authentication

One type of authentication prevailing in the networks today is group authentication [2] having further two types; (i) knowledge based authentication (passwords, etc.), and (ii) key based authentication. Knowledge based authentication has some flaws due to which passwords could be hacked. Key based authentication concerns with the computational time involved using large integers.

Data integrity and confidentiality

In networked society governmental decision making and public services are enhanced through increased use of ICT. But with increased network communication information became invasive and complicated interdependencies started to occur that gave way to various types of vulnerabilities. These vulnerabilities formed the basis for serious failures in critical infrastructures and introduced highly intrusive cyber-attacks. The ICT enabled countries are therefore giving high priority to counteract these threats.

Botnets provide platform for serious threats including distributed denial of service, information stolen and spamming. There are two complex scenarios been observed; there are stealthy botnet attacks that are hard to be identified, and legitimate P2P applications (e.g. skype, and bittorrent, etc.) are running on bot-infected hosts. Lastly, traffic analysis framework [3] is provided boosting scalability of botnet detectors being used. This framework can identify number of hosts that are botnet infected. But, the counter attack that would diminish these botnet infected attacks has not yet been realized.

Network Controlled Systems (NCS) [4] became vulnerable to attack in the presence of Internet and wireless communications delivering pervasive and non-proprietary information. Traditionally, when developing security mechanisms, the interdependencies between the physical systems and cyber connections in IT get ignored. Security in power systems should also be focused when creating security and reliability mechanisms for NCS.

Intrusive Behavior Detection and Prevention

It was recognized that automated intrusion detection and prevention [5] should be in place against intrusion attacks. Network traffic has to be continuously monitored through diagnostic systems for abnormal activity. Security scanning [6] should be performed at all sub-systems whether they are private enterprises or public cloud. Vulnerabilities found on enterprise computer systems can also be exploited by intruders reaching through open networks. When networking effective security architectures should assess the vulnerabilities found on the host. Cyber-crime is present to exploit network traffic to collect useful and private information. Intrusion detection tools are lacking to give full protection against these malicious attacks. Thus, developing effective tools is trivial job but to do this a test bed is required to represent a network and intruders attacks. But, monitoring or analyzing the network is not just sufficient unless the passive behavior being recognized is not blocked or discouraged. In this research, the importance is given to blockage and discouragement of intrusive occurrences.

Simulated Test Bed

A simulation [7] that was designed has been understood in this research to make another test bed with enhanced features. Also, Sridharan [8] discussed the vulnerabilities found in Smart Grid concept in 2012 during his research. These deficiencies gave way to intrusion in cyber space. Power system devices that are for managing and supplying electrical energy can be threatening to information sharing on the mobile networks. Till now there are no metrics formed to measure the threats and attacks on cyber networks. Sridharan proposed the test to measure the multiple-threat methods for monitoring cyber security on a multi-laboratory test bed that would assist in developing SCADA – a test bed devised at Georgia University, USA [8]. Thus, SCADA is also been analyzed in this study to come up with a well formed test bed which would enable standardized features like IPSec security protocol and intelligent routing mechanisms.

Knowledge Networks, Algorithms and Routing Protocol

It is been clarified in our problem statement that knowledge networks may be defined in four categories that are:

A. Sensor networks,
B. Mobile ad-hoc Networks (MANET)
C. Wireless networks, and
D. Semantic Web

Moving forward in our research it is necessary to understand the context of these network types and security considerations that are prevalent in these networks and measures been taken so far to add security.

ISSN:2319-7900

Sensor Networks

Sensor networks have been realized with the increasing use of wireless communications through electronic devices. The sensor networks are used within many scenarios (health, military, home, etc.). What is a sensor network? It is collection of several sensor nodes and its deployment is not predetermined [19]. Thus, requesting the algorithms and protocols engineered to tackle these sensor nodes must be intelligent enough to enable the nodes to manage themselves. The processors of sensor nodes are intelligent enough to preprocess the raw data and send only the required and partially processed data. Sensor networks do require wireless ad-hoc networking techniques. But there is a difference between ad-hoc networks and sensor networks. Main difference that would help distinguish the two is that ad-hoc networks is a point to point communication while sensor networks use broadcast communication and are densely deployed at higher orders of magnitude than the ad-hoc networks.

Time delays do occur during transmission in networked control systems. On exceeding the sample transmission time delay the system is considered unstable. This problem has been tried to be solved by introducing the logic-based fuzzy neural networks [24] for predicting the expected time delay. Using the predicted time delay sampling period of the networked control systems is determined. The transmission time delay data occurring in real systems has been tried to test and train the logic-based fuzzy neural networks.

Ionic bond-directed particle swarm optimization (IBPSO) [25] is proposed enhancing the particle swarm optimization (PSO) where ionic bond develops a close bond between two sensor nodes determining the node that has to move following a selected directed path while PSO solves a multidimensional function optimization in moving space. Through simulation it is been seen that IBPSO functions better than PSO for regional convergence and global searching and implements dynamic WSN deployment more rapidly in most efficient manner.

Mobile Ad-hoc Networks

As discussed earlier Knowledge networks are inclusive of Mobile Ad hoc Networks (MANETs). This is inclusive of autonomous self-organized nodes using wireless medium for connecting two ends for communication that are within each other transmission radius in a multi hop infrastructure. There has been progressive research been conducted in the past that proposed various routing algorithms for MANETs but the recent study shows the emerging trend in routing research is towards Swarm Intelligence (SI) [13].

Swarm Intelligence (SI) refers to an artificial intelligence technique [13] implemented on to a complex system that is meant to be decentralized and self-organized. It could result in observing intelligent and complex behavior emerging from simple unsupervised interaction of all swarm members part of a system or any network. There are various routing techniques based on Swarm Intelligence (SI) that are (i) Ant colony optimization (ACO) algorithm based routing protocols, and (ii) Bee colony optimization (BCO) based routing protocols. These algorithms are inspired by ants and bees behavior in their colonies. ACO based on ants characteristics of searching food is applied as such on MANETs for routing packets. The shortest path is found for routing packets. If it is found dead then an alternative path is utilized and likewise the routing packets adapt intelligently to the dynamically changing environment. Forwarded packets leave their track for following packets along the same path. ACO and BCO differ in their principles based on the different nature of ants and bees as ants walk and bees fly. As with ants, ACO lets the forwarding packets leave their trail behind them while in BCO, visual communication plays the same role. BCO based on bee characteristics works as a well-knitted team work, coordination, and simultaneous task performance. Here the tasks are allocated as per role of each packet being transmitted and respective protocols they follow as bees in their nature have defined behaviors according to their roles as queen bee, drones (males of the hives), worker bees termed as scout bees and forager bees. Such nature inspired routing protocols would be capable of removing at least one of several problems like; survivability, scalability, adaptability, maintainability, battery life, and further more.

Wireless Networks

Wireless communications [26] has gained momentum in the twenty first century. And, with the growth in cellular use, and other networks within businesses and homes the wireless communication has replaced wired networks. Every future appliance is coming with the wireless technology and being smart every day whether it is wireless sensor networks, automated highways and businesses, laptops and palmtops, and home appliances have all emerged in the recent researches. Now, the wireless communications network follow a highly successful IEEE standard i.e. IEEE 802.11 family of standards.

COPE [27] proposes architecture for wireless mesh network. It shows that intelligently packets mix gives high performance throughput. It is been practically tested on a 20-nodes wireless network. The performance depends on traffic pattern, transport protocol, and congestion level.

COPE encapsulates its own coding style between IP and MAC layers [27]. In an example (figure 2) it is simplified by showing the transmission between Alice and Bob through a router passing a pair of packets. In old scenario, Alice transmits a packet and router forwards it to Bob and vice

ISSN:2319-7900

versa. Thus, this flow of transmission requires 4 channels. In the coding approach of COPE, Alice and Bob both send their packets to the router and it in turn XORs the packets and broadcast the XOR-ed version of the packet. Now, Bob and Alice, both obtain their packets by XOR-ing again with their own packets. This mode of transmission limits the channels of communication to three instead of four.

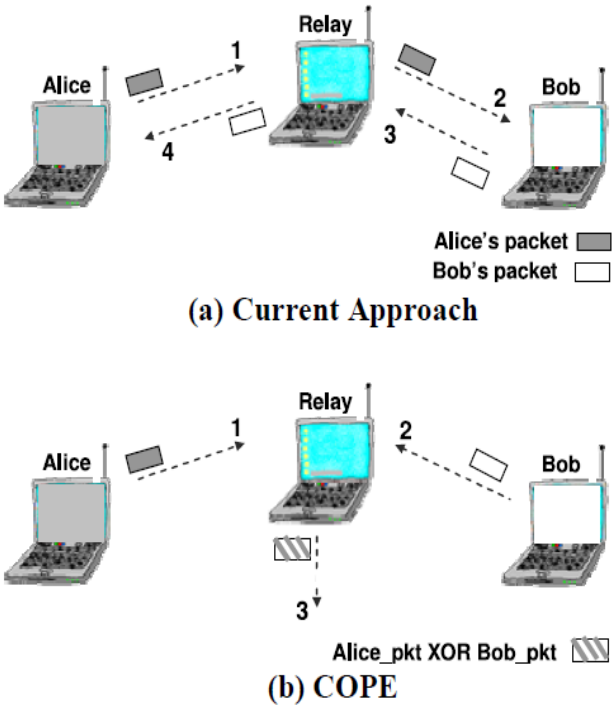


Figure 2. COPE Increasing Throughput by Limiting Transmission of a Pair of Packets to 3 Transmissions Rather 4 Transmissions [27]

Semantic Web

NetKAT[28] is a mathematical networking programming language for establishing semantic foundation. NetKAT design incorporates in itself the techniques for filtering, transmitting, and modifying packets. It uses a mathematically structured Kleene Algebra with tests (KAT) that is proved in its capacity for sound and complete equational theory catering substantial semantics. It is been practically implemented with syntactic techniques for reachability, non-interference properties implementation that isolates programs, and correct algorithm compilation is thus proved. It is thus established that the equational theory applied in several diverse domains provides reasoning while reaching, isolating traffic, and correct compilation.

Forwarding technique used in NetKAT is studied and packet details are known that includes fields for standard headers that have source address (src), destination address (dst), and protocol type (typ) and other two fields for switch (sw), and port (pt) that would identify the accurate location of the packet in the network.

Other atomic NetKAT techniques include filtering and modifying packets. A filter (f = n), would take any input packet pk yielding a singleton set {pk}, on condition if f (field) of pk (input packet) equals n and {} otherwise. Modifying (fn) gets input packet (pk) and yields singleton set {pk'} where pk' is the modified packet setting f to n.

Reach-ability properties are formulized based on questions like:

1. Does the intrusion detection system implied reaches all un-trusted traffic circulating the network?
2. Either all hosts communicate among themselves?, and
3. Whether managed hosts are kept isolated from un-managed hosts?

To cater to these problems an approach has been designed into NetKAT that show the encoding of two important classes of reach-ability properties within NetKAT equations. These equations are hence proved to be sound and complete being intuitive, semantically designed for reach-ability using its own language model.

For compilation [28] NetKAT program is executed on an OpenFlow switch and compiled using flow table, low level programming abstraction for which OpenFlow gives support. Prioritization is done in flow table based on list of rules where each rule has a pattern for matching packet headers and actions to other packets. Packet reaching a switch is catered as per highest priority matching rule.

Similarities and Differences of Knowledge Network

Table 1. Similarities and Differences among Four Types of Knowledge Networks

Characteristics	Deployment is not predetermined	Preprocessing data	Communication channels
Sensor Networks	Yes. Intelligently deployed	Yes. Partially processes data before sending to the desired destination	Broadcast
MANET	Self-organized	No preprocessing of data being transferred	Point-to-point
Wireless Networks	Yes. Nodes are always on move	No preprocessing	COPE architecture. Relay network
Semantic web	Servers are frequently being changed. IPs are not fixed	Extracting meaningful information	NetKAT algorithm. Forwarding packets through node to node

Proposed Network Design 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 [9]:

1. Confidentiality: data transmitted between two endpoints remains private
2. Integrity: the data does not get tampered during transmission
3. Availability: the endpoints are accessible whenever required
4. 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. With protocol compression where overhead is increased, the size of transmitted data has increased. Security duplication is avoided by providing cross-layer interaction between protocols. At network layer, Internet Protocol Security (IPSec) is implemented to keep the data exchange secure at different configuration parameters; (i) Gateway-to-gateway, (ii) Gateway-to-host, and (iii) host-to host communication [9]. IPSec is known for providing confidentiality, data-origin authentication, integrity and prevention against replay attacks. IPSec uses two security protocols; authentication header (AH), and Encapsulated Security Payload (ESP) used in combination with Internet key exchange (IKE).

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.

Cluster of Nodes

This 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 been proposed. This study gathers the most appropriate features of these and incorporates into a clustered network that enables monitoring in a dense network of nodes. Then:

1. Best and most appropriate security mechanisms are filtered through literature review and refined to integrate within the clustered network.
2. The knowledge networks are broken into dense clusters given some threshold parameters (e.g. area of each cluster).
3. 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.
4. It is being assumed that the base stations are already established to execute and monitor these clusters in a group.
5. Within each cluster there would be a cluster head that would be regulating the whole network traffic becoming part of the particular cluster.

Clustered Networks

Today large data centers consisting of tens of thousands of expensive elements like routers and switches catering to varied aggregate bandwidth requirements may support 50% of the total bandwidth at the edge of the network in a topology. And, the resulting cost would also be maximum depending on the topology. Varied bandwidth among the networks complicates the arrangement and design of networks and overall system performance [10].

Thus, study [10] is done to develop clusters for getting full aggregate bandwidth out of network topology in large data centers having tens of thousands of nodes. It is argued that proper installation and design of network switch-

ISSN:2319-7900

es/routers would give high performance with minimal cost. The proposed approach needs no modification on the end host network interface and is fully compatible with IP, Ethernet, and TCP.

The routing algorithm [10] used is taken from the previously proposed architecture built with first two levels of switches acting as filters for traffic diffusers, the upper and lower end switches in a given pod implements prefixes to terminate subnets of that pod.

So if a host sends a packet to the destination within same pod but having different subnet the terminating prefix would be pointing to the destination subnet's switch. The core switches have the terminating first-level prefixes for all network IDs pointed to the right pod containing that specific network. Thus, a single path is established between the core switch and the destination pod. To keep it simple it is assumed that a central entity has full knowledge of the interconnected cluster topology.

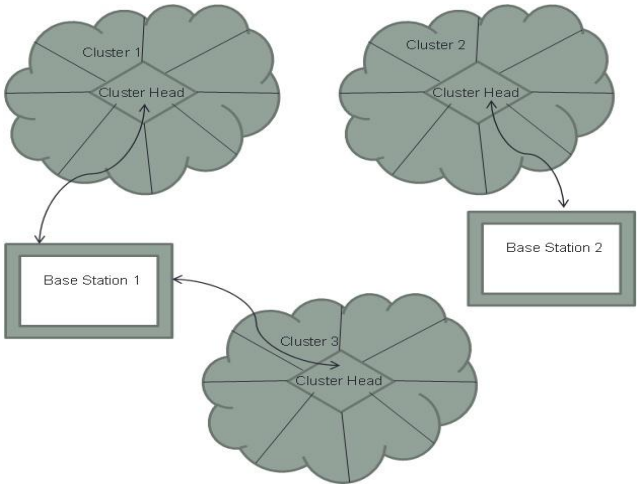


Figure 3. Clustered Network Design Having a Cluster Head

Power Centric Nodes

Systems running on a power supply are also known to be threatening to knowledge networks as they are known to be sharing informative data along the network channel. As this research already clarifies Sridharan's[8] 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 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 been maintained as well when creating a robust network [4]. As there were mechanisms formed for security of NCS such optimal solution is designed to protect routers and gateways too, sensing the malicious data corruption attacks in information channels connecting routers and within the routers itself. Then there is centralized host-based security scanning architecture [6] that is also made part of the routers within a cluster.

Monitoring for Intrusive Activities

Boost-up Botnet detection system [3] is there contributing three novel strategies for tackling the cyber-attacks like; drive-by download attacks that were missed before by existing detectors, then there is P2P Command & Control (C&C) structures adopted to identify attacks that could be disrupt the network. Finally, a framework is provided for traffic analysis to boost the effectiveness of botnet detection system. Algorithms for adaptive packet sampling and novel botnet aware system are there with scalable flow-correlation technique. Network Intrusion Detection Systems (NIDS), and Network Intrusion Prevention Systems(NIPS) are inbuilt in central network connecting devices such as routers (nodes) integrating them with the tool called Multistage Attack Recognition System (MARS) [5] that includes a collection of integrated components: alert correlation, graph reduction, and alert aggregation.

HADM-KRS

Two versions that are proposed [11] for the high availability of decentralized cryptographic multi-agent key recovery system (HADM-KRS) are employed that completely comply with the NIST framework for the latest key recovery system. System administrators are able to specify minimum number of key recovery agents (KRAs) 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.

IPSec Security Protocol

IPSec[12] is a standard security protocol 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 is done on outgoing packets being sent to network. And, thus incoming packets are decrypted, de-capsulated and verified upon receipt. Key management in this system is simpler.

Design of encapsulation techniques for basic authentication and confidentiality is not that difficult and IPSec is standardized by IETF and implemented by commercial vendors.

Standardization

ISSN:2319-7900

The security mechanisms being implemented would be validated mapping onto the cyber security standards as implemented by IETF and NIST.

Proposed Algorithm for iRoutCluster Protocol

This research caters to attending the knowledge networks inclusive of; (i) Sensor Networks, (ii) Mobile Ad-hoc Networks (MANETs), (iii) Wireless Networks, and (iv) Semantic Web. The Intelligent Routing Cluster (iRoutCluster) protocol designed to be implemented in this research is such that it would be covering all four domains of knowledge networks discussed in this research. Mainly it is influenced by Bee colony optimization (BCO) based routing protocols that is itself a Swarm Intelligence (SI) based technique for networking [13]. As BCO itself keeps a nature of bees in real life scenario so it could be implemented in all types of knowledge networks. There is already many protocols been implemented for MANETs but it is specifically good to utilize for wireless, sensor and semantic web networks.

The enhancement is made in adapting to a clustered network. Where a center point (cluster head) is already been established that in turn is responsive to the base station executing it. These clusters would be having all four domains of network connections and iRoutCluster is intelligent enough to respond towards each one. iRoutCluster would be made responsible for all communications taking place within a respective cluster and it would intelligently keep track of end to end communication. It would be supported by IPSec protocol [12] being embedded with it into the network that would be responsible for gateway-to-node communication. And, IPSec security protocol is also applicable at all levels of knowledge networks.

Utilizing the BCO visual monitoring feature, the iRoutCluster enables the cluster head to take snapshots of the operating system within the nodes that are included in its range. These snapshots are simultaneously being visualized by base stations at very detail level. Thus, the network design captures every minute detail of malfunctioning in the knowledge networks that is composed of sensor networks, mobile ad-hoc networks, wireless networks, and semantic web.

iRoutCluster complying with Knowledge Networks

In the previous section, we have already studied the similarities and difference between four types of knowledge networks that are being considered in this study. Now, there is need to realize the mechanism of iRoutCluster to be compliant with all four knowledge networks domains spread between sensor networks, MANETs, wireless networks and semantic web.

Deployment is not pre-determined

We have already realized that all four type of knowledge networks are intelligently deployed and are self-organized. iRoutCluster as understood follows the swarm intelligence technique using BCO routing protocols that are themselves quite intelligent in organizing the nodes through visual sensing and feeling the movement of other nodes in the same network. Plus, iRoutCluster is a mix of protocols leveraged from these networks. It is inclusive of COPE and NetKAT algorithms to enhance its capabilities in managing between broad spectrums of knowledge networks.

Pre-processing Data

It is known that sensor networks and semantic web use preprocessing techniques for partially or somewhat extracting meaningful interpretation over the web. This feature is provided in iRoutCluster as it is inclusive of NetKAT and the sensor nodes in sensor networks are already been controlled via processors having inbuilt capability of preprocessing data.

Communication Channels

Communication whether it is broadband or point-to-point is managed by authorizing through tokens of various type. If a node or server is about to broadcast it would circulate the broadcast token to its member nodes that has to be reached and other nodes would be kept isolated from this broadcast. Likewise if there is point-to-point communication taking place the token keys would be shared among the two nodes that need to communicate and understood by only these two nodes. If there is a relay channel then the packets would be transmitted using COPE algorithm.

Security

Knowledge networks inclusive of four domains being discussed are kept secured using IPSec protocol and HADM-KRS in compliance with IETF and NIST standards. Plus, Network Intrusion Detection Systems (NIDS), and Network Intrusion Prevention Systems are inbuilt in central network connecting devices such as routers (nodes) integrating them with the tool called Multistage Attack Recognition System (MARS) [5] that includes a collection of integrated components: alert correlation, graph reduction, and alert aggregation.

Experimental Setup

ISSN:2319-7900

A simulation [7] for producing real-time network traffic is adopted that generated test data and cyber-attacks in presence of security intrusion detection systems. The security protocol being used is IPSec on each router in the network.

A simulated network design (figure 4) is thus proposed to hold power centric intelligent nodes (routers) within clustered knowledge networks. In real network system, the clusters would be formed such that each town or city would have one intelligent cluster.

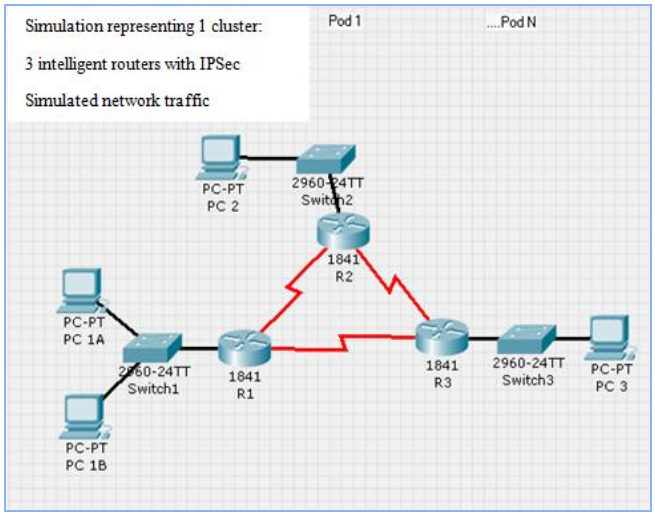


Figure 4. A Networked Cluster Simulation Having 3 Intelligent Routers

Other two simulations for wireless sensor networks are done using MATLAB to relate "hop count" with "network size" estimate (figure 5). This is the way each cluster of nodes would relate itself to the other cluster (figure 6) in terms of "hop count" and within a certain "response time" (figure 7). Then figure 8 is there to validate the network against success rate that is achieved keeping a considerable network size in a cluster.

This set of multiple experiments and simulations to test and validate the success rate of response and hop time for various networks within clusters of 10 to 20 nodes has been found enough for getting the desired result that is shown in above figures.

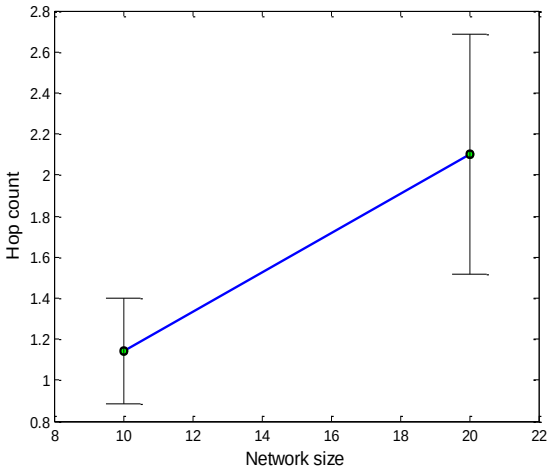


Figure 5. Hop Count Against Network Size of Each Cluster

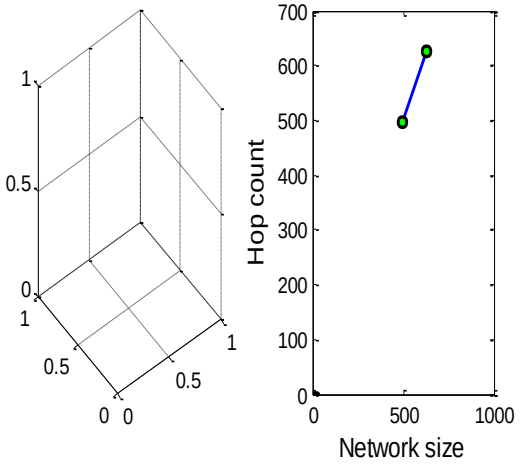


Figure 6. Linking Hop Counts Between Clusters (3D and 2D view)

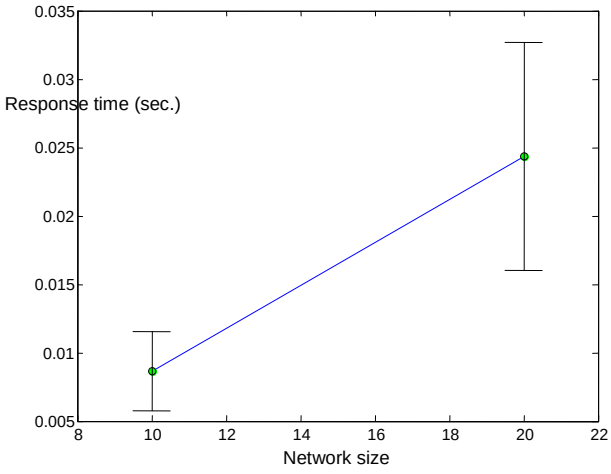


Figure 7. Calculated Response Time Between Two Clusters

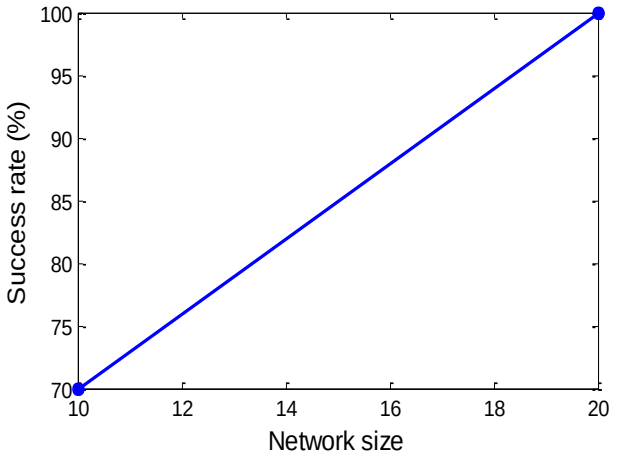


Figure 8. Success Rate Achieved Keeping Limited to a Considerable Network Size within Cluster

Conclusion

Finding an optimum solution to 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 endangers this massive network. Therefore, standardized measures have been experimented and adopted for better results and future considerations to implement them in real scenarios. IPSec protocol is implemented as it is standardized by Internet Engineering Task Force (IETF) already been 70% implemented. Any future development towards knowledge networks would require a strong foundation that could not be outperformed by security threats. It would be thoroughly tested against current penetration techniques employed by intruders. 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.

A recovery system has also been tried and implemented that complies with latest NIST framework known for high availability of decentralized cryptographic multi-agent key recovery system (HADM-KRS).

Also, after exhaustive testing experimental results of multiple simulations the conclusion has been reached to create clusters of up to 10 to 20 nodes corresponding with intelligent routers in place for getting the desired success in monitoring the activities of nodes within a cluster. The average success rate after evaluating the response time and hop count of a considerable network size it is been viewed that nodes between 10 to 20 give the optimal result or otherwise the cluster would grow too large to manage and keep track of.

References

[1] A. Lindgren, A. Doria, & O. Schelen, "Probabilistic routing in intermittently connected networks", *ACM, Electronics and Telecommunications Research Institute (ETRI)*, Korea, 2004.

[2] L. Harn, & C. Lin, "An efficient group authentication for group communications", *International Journal of Network Security & Its Applications (IJNSA)*, Vol.5, No.3, May 2013

[3] J. Zhang, "Effective and Scalable Botnet Detection in Network Traffic", PhD, Georgia Institute of Technology, 2012.

[4] A. Teixeira, "toward secure and reliable Networked Control Systems", Master's Thesis, KTH Royal Institute of Technology, 2011.

[5] F. Alserhani, "A framework for correlation and aggregation of security alerts in communication networks", PhD, University of Bradford, 2011.

[6] A. Rakshit, "A host-based security assessment architecture for effective leveraging of shared knowledge", Master's thesis, Kansas State University, India, 2009.

[7] K. Costantini, "Development of a Cyber Attack Simulator for Network Modeling and Cyber Security Analysis", Master's thesis, Rochester Institute of Technology, 2007.

[8] V. Sridharan, "Cyber Security in Power Systems", Master's Thesis, Georgia Institute of Technology, 2012.

[9] S. Cirani, G. Ferrari, and L. Veltri, "Enforcing security mechanisms in the IP-based internet of things: An algorithmic overview", *Algorithms 2013*, Vol. 6, 197-226, 2013

[10] M. Al-Fares, A. Loukissas, & A. Vahdat, "A scalable, commodity data center network architecture", *SIGCOMM'08*, Seattle, Washington, USA, 2008.

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

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

[13] C. Raghavendran, G. Satish, & P. Verma, "Intelligent routing techniques for mobile ad hoc networks using swarm intelligence", *I. J. Intelligent Systems and Applications*, India, 2013.

[14] R. Reddy, "Personal Knowledge Networks in the Mobile Millennium", Proc. *IEEE International Sym-*

ISSN:2319-7900

posium on IT in medicine and education, West Virginia Uni., USA, 2009

[15] S.Nousala, "Understanding the value and transference of tacit knowledge in socio-technical networks and complex systems: a study of simultaneous internal and external organizational knowledge networks", Proc. 8th international conference on ITST, RMIT, Australia, 2008.

[16] M. Newman, "The structure and function of complex networks", University of Michigan, USA, 2003.

[17] L. Li, D. Alderson, W.Willinger, & J. Doyle, "A first-principles approach to understanding the Internet's router-level topology", *SIGCOMM'04*, Portland, Oregon, USA, 2004.

[18] D. Andersen, H. Balakrishnan, F. Kaashoek, &R. Morris, "Resilient Overlay Networks", Proc. *18th ACM Symp. on Operating Systems Principles (SOSP)*, Banff, Canada, October 2001.

[19] I. Akyildiz, W. Su, Y. Sankarasubramaniam, &E. Cayirci, "A Survey on sensor networks", *Communications Magazine, IEEE* Vol. 40 , No. 8, pp. 102-114, 2002.

[20] S. Marti, T.Giuli, K. Lai, & M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", Stanford University, USA, 2000.

[21] B. Karp & H. Kung, "GPSR: Greedy Perimeter Stateless Routing for wireless networks", MobiCom 2000, Harvard University, 2000

[22] I. Clarke, O. Sandberg, B. Wiley, & T. Hong, "Freenet: A distributed anonymous information storage and retrieval System", *National Science Foundation and Marshall Aid Commemoration Commission*, 2001.

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

[24] C. Han, "Fuzzy Neural Network-Based Time Delay Prediction for Networked Control Systems", *Applied Mathematics and Information Sciences*, Vol. 8 (No. 1), 407-413, 2014

[25] H. Huang, J. Zhang, R. Wang, & Y.Qian, "Sensor Node Deployment in Wireless Sensor Networks based on Ionic Bond-Directed Particle Swarm Optimization", *Applied Mathematics and Information Sciences*, Vol. 8 (No. 2), 597-605, 2014

[26] A. Goldsmith, "Wireless Communications", Stanford University, USA., 2005

[27] S.Katti, H. Rahul, W. Hu, D.Katabi, M.Medard, & J.Crowcroft, "XORs in the air: Practical wireless network coding", *SIGCOMM'06*, Pisa, Italy, 2006.

[28] C. Anderson, N. Foster, A.Guha, J.Jeannin, D.Kozen, C. Schlesinger, & D. Walker, "NetKAT: Semantic Foundations for Networks", *POPL '14, ACM*, January 22–24, San Diego, CA, USA., 2014

[29] H. Tangmunarunkit, R. Govindan, S. Jamin, S. Shenker, and W. Willinger. Network Topology Generators: Degree-Based vs. Structural, In *Proc. ACM SIGCOMM 2002*.

[30] M. Roughan, A. Greenberg, C. Kalmanek, M. Rumsewicz, J.Yates and Y. Zhang. Experience in Measuring Backbone Traffic Variability: Models, Metrics, Measurements and Meaning *International Teletraffic Congress (ITC)* 18, 2003.