International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Distributed Intrusion Detection System for Cognitive Radio Networks Based on Weighted Fair Queuing Algorithm

[1]M. Indhumathi, [2]S. Kavitha

[1]Research Scholar, Department of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram, India
[2]Head & Associate Professor, Department of Computer Science, Sakthi College of Arts and Science For Women, Oddanchatram, India

ABSTRACT

Reliable detection of intrusion is the basis of safety in cognitive radio networks (CRNs). So far, few scholars applied intrusion detection systems (IDS) to combat intrusion against CRNs. In order to improve the performance of intrusion detection in CRNs, a distributed intrusion detection scheme has been proposed. In this paper, a method base on Dempster-Shafer's (DS) evidence theory to detect intrusion in CRNs is put forward, in which the detection data and credibility of different local IDS Agent is combined by D-S in the cooperative detection center, so that different local detection decisions are taken into consideration in the final decision. The effectiveness of the proposed scheme is verified by simulation, and the results reflect a noticeable performance improvement between the proposed scheme and the traditional method.

Keywords : Safety, cognitive radio networks, intrusion detection, IDS Agent, cooperative detection center, Dempster-Shafer's evidence theory

I. INTRODUCTION

1.1 INTRODUCTION ABOUT TO IDS

1.1.1 IDS Defined

Intrusion detection is the process of identifying computing or network activity that is malicious or unauthorized. Most all Intrusion Detection Systems (IDS) have a similar structure and component set. This consists of a sensor (or agent) that monitors one or more data sources, applies some type of detection algorithm, and then initiates zero or more responses. Usually there is a management system that provides for monitoring, configuration and analysis of intrusion data.

1.1.2 Evolution of IDS

The first IDS were host-based, and looked at system operating logs performing simple pattern matches against a small set of signatures. This approach quickly expanded to systems that looked at network traffic, initially also for simple patterns. As IDS gained a level of protocol-awareness, they were able to look for certain single packet traffic types known to be malicious, examining the source and destination IP addresses, along with source and destination ports. Further sophistication brought an awareness of network sessions and the ability to examine dialogs between systems for multi-packet activity. More recent IDS can examine and respond to entire conversations between hosts, using knowledge of protocols and network sessions to analyze traffic for malicious activity based on how that traffic would appear at the destination-a task often requiring specialized network drivers to operate at full wire-speed (For a good discussion of the evolution and genealogy of IDS, see article by Inella). The emerging class of IDS take this one step

further by combining log analysis, along with information from other IDS and anti-virus software to correlate events in an effort to identify and respond to intrusions in real time.

1.1.3 Relation of IDS to dIDS

From the above, it is clear that as IDS grow in function and evolve in power, they also evolve in complexity. Agents of each new generation of IDS use agents of the previous generation as data sources, applying ever more sophisticated detection algorithms to determine ever more targeted responses. Often, one or more IDS and management system(s) may be deployed by an organization within its own network, with little regard to their neighbors or the global Internet. Just as all individual networks and intranets connect to form "The Internet", so can information from stand-alone

A secure computer system provides guarantees regarding the confidentiality, integrity, and availability of its objects (such as data, purpose, or services). However, systems generally contain design and implementation flaws that result in security vulnerabilities. An intrusion can take place when an attacker or a group of attackers exploits the vulnerabilities and thus damages the confidentiality, integrity or availability guarantees of a system. Intrusion Detection Systems (IDSs) detect some set of intrusions and execute some predetermined actions when an intrusion is detected. Over the last one and half decade, research in the field of intrusion detection has been heading towards a distributed framework of systems that do local detection and provide information to perform global detection of intrusions.

These distributed frameworks of intrusion detection have some advantages over single monolithic frameworks. Most of these distributed systems are hierarchical in nature. The local intrusion detection components look for local intrusions and pass their analysis results to the upper levels of the hierarchy. The components at the upper levels analyze the refined data from multiple lower level components and attempt to establish a global view of the system state. However, such IDSs are not fully distributed systems because of the centralized data analysis performed at the higher levels of the hierarchy. An agent-based architecture is proposed for performing intrusion detection in a distributed environment. By employing a suitable communication mechanism, the resource overhead is minimized in the distributed intrusion detection process.

1.2 INTRODUCTION TO DIDS

Some of the existing distributed IDS frameworks are discussed briefly. DIDS is a distributed intrusion detection system consisting of host managers and LAN managers doing distributed data monitoring, and sending notable events to the DIDS director. These managers also do some local detection, passing the summaries to the director. The director analyzes the events to determine the security state. AAFID is distributed IDS developed in CERIAS at Purdue University. It employs agents at the lowest level of the hierarchy for data collection and analysis and transceivers and monitors at the higher levels for controlling agents and obtaining a global view of activities. It provides a subscription-based service to the agents.

A prototype called the Hummingbird System is developed at University of Idaho. It is a distributed system that employs a set of Hummer agents, each assigned to a single host or a set of hosts. Each Hummer interacts with other hummers in the system through a manager, a subordinate, and the peer relationships. It enables a system administrator to monitor security threats on multiple computers. Architecture of an intrusion detection system using a collection of autonomous agents has been proposed in. In cooperation and communication model proposed by the authors, agents request and receive information solely on the basis of their interests. They can specify new interests as a result of a new

event or alert. This avoids unnecessary data flow among the agents.

However, most of these intrusion detection systems have the following drawbacks: (i) **Analysis hierarchy**: as there is a hierarchy in data analysis these systems are very difficult to modify. Changes may have to be made at many levels if any new distributed attack is developed. (ii) **Data refinement**: when a module from a lower level sends results of analysis to a higher level, some data refinement is done. However, the knowledge of what events are important in a system-wide level is difficult to anticipate at the lower levels of the hierarchy, and thus data refinement may result in loss of important information.

1.3 Wireless Sensor Networks Applications

Figure-1: Wireless Sensor Networks Applications

(i) These networks are used in environmental tracking, such as forest detection, animal tracking, flood detection, forecasting and weather prediction, and also in commercial applications like seismic activities prediction and monitoring.

(ii) Military applications, such as tracking and environment monitoring surveillance applications use these networks. The sensor nodes from sensor networks are dropped to the field of interest and are remotely controlled by a user. Enemy tracking, security detections are also performed by using these networks.

(iii) Health applications, such as Tracking and monitoring of patients and doctors use these networks.

(iv) The most frequently used wireless sensor networks applications in the field of Transport systems such as monitoring of traffic, dynamic routing management and monitoring of parking lots, etc., use these networks.

(v) Rapid emergency response, industrial process monitoring, automated building climate control, ecosystem and habitat monitoring, civil structural health monitoring, etc., use these networks.

Wireless Sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes. A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). To prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. In this paper, for convenience, we call this sort of cluster-based protocols as LEACH-like proto-cols. Researchers have been widely studying CWSNs in the last decade in the literature.

The multi-constrained QoS routing is NP-hard and heuristic algorithms are proposed to find solution for the problem. But these algorithms are too complex and cannot obtain best global solution. QoS may be more accurately determined by using fuzzy logic instead of static values. Fuzzy Inference System (FIS) accepts more number of uncertain and imprecise data as inputs and thereby achieves flexibility, robustness, and low cost solution. But, FIS uses human-determined membership functions (MFs) that are fixed. Therefore, they are rarely optimal in

terms of reproducing the desired outputs. Tuning membership functions of parameters is a time consuming task. Neural networks overcome most of the complex problems to adapt dynamically to the system operating conditions, and to make correct decisions, if the signals are uncertain. But the integration of neural network into the fuzzy logic system makes it possible to learn from prior obtained data sets. This paper proposes an approach which integrates both neural and fuzzy techniques to select a server from a number of group members belonging to any cast group by considering QoS constraint route and server with higher stability in MANETs. This section presents some of the related works, software agent concept and our contributions.

The set of destinations is identified by unique any cast address and provide the same services. Searching for services on networks often depends on the broadcast or multicast mechanism to acquire the information, which usually results in large overhead. It will be a serious problem in ad-hoc wireless networks, where the bandwidth is limited and each node moves arbitrarily. Any casting scheme in ad hoc wireless networks can simplify access management in distributed service, improve the robustness and performance of an ad hoc network when mobility and link disconnections are frequent, and reduces the communication overhead.

The source node does not need to know about picking a single server and is determined by routing scheme. The server in any cast routing may be chosen by minimum hops, delay or other metrics. Any casting along the minimum hops path may result in inefficient use of network resources, because it forwards packets along already congested shortest path, and also may not satisfy the Quality of Service (QoS) requirements for multimedia and real time application services. Set of mobile or semi mobile nodes with no available pre-established communications is a MANET Forming a short-term network. Each mobile node in the network acts as a computer switching program that transfers incoming messages to outgoing links via the most efficient route possible, e.g. over the Internet i.e., a router. This kind of networks are characterize by the relationships between parts linked together in a system such as a computer network topologies, continuation of bandwidth constrain and variable capacity links, energy constrain operations and are highly intensity to security threats. Due to all these characteristics routing is a major issue in ad hoc networks. The routing protocols for ad hoc networks have been classified as: (a) Proactive or table driven for example Destination Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OLSR), (b) Reactive/On-demand, e.g. Dynamic Source Routing Protocol, Ad hoc On-Demand Distance Vector routing protocol, Temporally Ordered Routing Algorithm. In table driven or proactive routing, each node has one or more tables that include the latest information of the routes to any node in the network. Each row has the subsequently hop for reaching to a node or subnet and the cost of this route. Different table-driven protocols vary in the way the information about alter in topology is spread through all nodes in the network. The two kinds of table keep informed in proactive protocols are the periodic update and the triggered update.

1.4 COGNITIVE RADIO NETWORK

Cognitive radio (CR) is a form of wireless communication in which a transceiver can intelligently detect which communication channels are in use and which are not, and instantly move into vacant channels while avoiding occupied ones. This optimizes the use of available radio-frequency (RF) spectrum while minimizing interference to other users.

In its most basic form, CR is a hybrid technology involving software defined radio (SDR) as applied to spread spectrum communications. Possible functions of cognitive radio include the ability of a transceiver to determine its geographic location,

identify and authorize its user, encrypt or decrypt signals, sense neighboring wireless devices in operation, and adjust output power and modulation characteristics.

II. LITERTURE REVIEW

Jaydip Sen, A Survey on Wireless Sensor Network Security [1] Wireless sensor networks (WSNs) have recently attracted a lot of interest in the research community due their wide range of applications. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. This problem is more critical if the network is deployed for some mission-critical applications such as in a tactical battlefield. Random failure of nodes is also very likely in real-life deployment scenarios. Due to resource constraints in the sensor nodes, traditional security mechanisms with large overhead of computation and communication are infeasible in WSNs. Security in sensor networks is, therefore, a particularly challenging task. This paper discusses the current state of the art in security mechanisms for WSNs. various types of attacks are discussed and their countermeasures presented. A brief discussion on the future direction of research in WSN security is also included. In addition to traditional security issues like secure routing and secure data aggregation, security mechanisms Deployed in WSNs also should involve collaborations among the nodes due to the decentralized nature of the networks and absence of any infrastructure. In real-world WSNs, the nodes cannot be assumed to be trustworthy apriori. Researchers have therefore, focused on building a sensor trust model to solve the problems which are beyond the capabilities of traditional cryptographic mechanisms. In this chapter, we present a survey of the security issues in WSNs. First we outline the constraints of WSNs, security requirements in these networks, and various possible attacks and the corresponding countermeasures. Then a holistic view of the security issues is presented. These issues are classified into six categories: cryptography, key management, secure routing, secure data aggregation, intrusion detection and trust management. The advantages and disadvantages of various security protocols are discussed, compared and evaluated. Some open research issues in each of these areas are also discussed.

Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR based Dynamic Clustering Mechanisms [2] Advances in Wireless Sensor Network Technology (WSN) have provided the availability of small and low-cost sensor with capability of sensing various types of physical and environmental conditions, data processing and wireless communication. In WSN, the sensor nodes have a limited transmission range, and their processing and storage capabilities as well as their energy resources are limited. Triple Umpiring System (TUS) has already been proved its better performance on Wireless Sensor Networks. Clustering technique provides an effective way to prolong the lifetime of WSN. In this paper, we modified the Ad hoc on demand Distance Vector Routing (AODV) by incorporating Signal to Noise Ratio (SNR) based dynamic clustering. The proposed scheme Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR based dynamic Clustering mechanisms (ESRPSDC) can partition the nodes into clusters and select the Cluster Head (CH) among the nodes based on the energy and Non Cluster Head (NCH) nodes join with a specific CH based on SNR Values. Error recovery has been implemented during Inter cluster routing itself in order to avoid end-to-end error recovery. Security has been achieved by isolating the malicious nodes using sink based routing pattern analysis. Extensive investigation studies using Global Mobile Simulator (GloMoSim) showed that this Hybrid ESRP significantly improves the Energy efficiency and Packet Reception Rate (PRR) compared to SNR unaware routing algorithms like Low Energy Aware Adaptive Clustering Hierarchy (LEACH) and Power-Efficient Gathering

in Sensor Information Systems (PEGASIS). Sensor Network Wireless is widely considered as one of the most important technologies for the twenty-first century. The sensing electronics measure ambient conditions related to the environment surrounding the sensors and transform them in to an electrical signal. In many WSN applications, the deployment of sensor

III. METHODOLOGY

(i) Security Agents

3.1. Misuse Detection Agent

As we previously mentioned, each security agent consists of two tiers. The lower tier comprises of the process that handles the misuse detection within our network. Snort [6] has been chosen as the misuse IDS software for our system. Snort is a libpcap-based [7] software that can be used as a sniffer, packet logger or network intrusion detection system. In our case, we used Snort as a misuse intrusion detection tool. The detection of malicious packets is based on known attack signatures. Snort is able to detect a variety of attacks such as DoS/DDoS attacks, Portscans, HTTP, DNS, SMTP, IMAP, POP3 attacks and Virus/Worm attacks.

Alerts generated from Snort are passed to the upper tier of our agent. The upper tier of the Misuse Detection Agent receives alert messages from the lower tier and stores them for a defined period of time in a buffer. For every different case of attack, that is, source IP address and port, target IP address and port and known attack signature, the upper tier process uses a unique alert identification. Rate limiting is achieved independently for different types of attacks, sending the alert message only once in the specified period of time.

Agent's upper tier process is also responsible for sending the heartbeat messages to the Central IDS Node informing that the misuse IDS system is operational. The messages sent to the Central IDS Node are formatted using the extended signed IDMEF format. In addition, the upper tier process listens for commands from the Central IDS Node. It receives parameters for the rate limiting of alert messages, configuration for the Snort process and new attack signatures.

3.2. Anomaly Detection Agent

For the lower tier of the Anomaly Detection Agent we developed a prototype anomaly detection tool [8] that currently focuses on DoS Attacks. The prototype tool consists of two main modules: the collector and the detector. The collector module is responsible for asynchronously receiving flow data from the Netflow-enabled [9] router; information is analyzed, mean values and adaptive thresholds are calculated and stored in a local data structure.

The tool extracts and stores packet and flow counters per destination IP address, as well as total counters and mean values for each pair of input-output interfaces. The detector process is responsible for calculating the metrics for the interface pairs stored by the collector, and comparing the results to detection thresholds. It is periodically activated, implements extensive logging of detection events and generates notifications with security alerts which are sent to the upper tier.

The upper tier process receives the alerts and sends them to the Central IDS Node using the signedIDMEF Format. Moreover, the Central IDS Node adjusts Anomaly Detection Agent's parameters (metrics and thresholds for the DoS attack detection algorithm).

3.3. SNMP Query Agent

As the other two agents, the SNMP Query Agent is comprised of two tiers. The lower tier process is a

custom SNMP client that performs SNMP queries at the routers of the network. Values like CPU and memory usage, active and inactive flows are polled from routers at specific intervals. The upper tier accepts the values from the SNMP queries and forwards them to the Central IDS Node after formatting them using the signed-IDMEF data model. The upper tier process is also responsible for sending heartbeat messages to inform the Central IDS Node that the SNMP client is operational. Instructions from the Central IDS Node are sent to the SNMP Query Agent, giving information about the router and the SNMP objects to be polled.

(ii) Intrusion Detection System

Intrusion detection mechanism can detect malicious behavior on the network and identify malicious users. So Intrusion detection mechanism can protect the reliability of the network, especially it is more important in distributed cognitive radio network which absenting center facilities. The traditional intrusion detection system (IDS) was proposed by Denning in 1987. It is composed of main body, object, audit record, activity profile and exception record and activity rules. A more detailed description of IDES is given as follows.

There are six main parts in the IDS model [12].

1) Subject: Active initiator in the system operation, the entity that moves on the target system, such as the process of the computer operating system, the service connection of the network and so on.

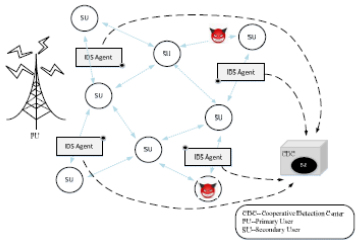

Figure-2:. System of Distribute Intrusion Detection in CRNs

2) Object: Resources that are managed by the system-- files, devices, commands, for example.

3) Audit Records: when a subject operates on an object, such as user registration, command execution, and file access, data will be produced by the target system.

4) Activity Profile: Preserve the information about the normal activity, and the specific implementation depends on the detection method.

5) Anomaly Record: Used to indicate the occurrence of an abnormal event. The format is <Event, Time-Stamp, Profile>

6) Activity rule: An action that should be taken when an audit record, update profile, an exception record, detect relate anomalies to some suspected intrusions or abnormal behavior is produced.

Actually, the Denning model is can be described as a rule based pattern matching system. After generating an audit record, it will match against the profiles. Then type information will determine the rule to report anomalies detection. It's largely system-in-dependent for the rules and profile structures to establish profile templates. Not all of the IDS can be fully consistent with the model.

IV. CONGESTION CONTROL FOR WIRELESS SENSOR NETWORK

4.1 Congestion Control

The flow type is of high importance to guide a real congestion control. Flow types may include a single packet, few packets, a large number of packets, which require light control, medium level control, and tight control, respectively. When a large number of nodes transmit information, their flows will cross at intermediate nodes. This high number of sources increases the congestion but helps improving the reliability. For example, in tree architectures, every intermediate node can suffer from congestion causing packet loss, which in turn decreases network performance and throughput and cause energy waste. It is very difficult to predict the intersection points due to network dynamics (addition or removal of sensors or a change in the report rate), variability in radio channel quality over time. All these can

transform uncongested parts of the network to under-provisioned and congested regions. The area around the intersection will become a hotspot and there is a possibility of congestion (buffer overflow) and contention (links interference). For these reasons, a congestion control algorithm for data packet transmission is necessary.

Contention-based Congestion: when many nodes within range of one another attempt to transmit simultaneously, losses occur due to interference and packet loss is engendered. If the packet generation rate is sufficiently small, simultaneous transmission becomes independent of the rate. Rather, it depends on the exact time generation of the packet. Explicit local synchronization (or also named phase shifting) among neighbours can reduce this type of loss, but it cannot eliminate the problem as non-neighbouring nodes can still interfere (hidden nodes). The contention may happen between different flows in the same area, and between different packets of the same flow, especially in the case of high density networks. Consequently, the nodes' channel capacity becomes time-variant. Buffer-based Congestion: each node uses a buffer for the packets waiting to be sent. The overflow of this buffer causes congestion and packets loss. This is due to high reporting rate that varies in time due to dynamic channel conditions. The many-to-one nature (or converge cast) of WSNs causes congestion, in addition to the other causes shared with general wireless networks.

4.2 Congestion Detection Strategies

Many congestion detection mechanisms are used and tested. The most used are: packet loss, queue length, packet service time, the ratio between packet service time and packet inter-arrival time, delay. In many cases, a single parameter cannot indicate congestion accurately.

Packet loss: It can be measured at the sender if ACKs (Acknowledgements) are used; this suggests reliability to be ensured by the protocol. It can also be measured at the receiver with sequence numbers use. Further, CTS (Clear To Send) packet loss can be used as congestion indication.. Not overhearing the parent's forwarding on the upstream link, by a child node over the downstream link, can be used as an indication for packet loss as well. The time to repair losses (if reliability ensured) can be used as a congestion indication. Loss ratio is also used in some protocols.

Queue length: As each node has a buffer; its length can serve a simple and good indication of congestion a fixed threshold is used and the congestion is signalled as soon as the buffer length exceeds this threshold , the remaining buffer length from the overall size is used. In the difference between the remaining buffer and the traffic rate is used as congestion indication. The traffic rate represents the excess rate, which is the difference between the output rate and the sum of sourced and forwarded rates. In the buffer length is used in addition to the difference of output and input time, which is quite similar to output and input rate. In buffer length and capacity of the node are used together. The number of non-empty queues can indicate congestion level. When there is a congestion, this number is larger than 0. This number increases with network load. If the link layer applies retransmissions, link contention will be reflected through buffer length.

Queue length and Channel load: In case of increase in packets collision, and after several unsuccessful MAC (Medium Access Control) retransmissions, packets are removed. Consequently, the decrease in buffer occupancy due to these drops may mean the absence of congestion when only buffer state is used for congestion detection. Therefore, for accurate congestion detection, a hybrid approach is required using queue length and channel loading as a congestion indication. Channel busyness ratio or channel load is the ratio of time intervals when the channel is busy (successful transmission or collision) to the total time. In the authors use the busyness channel ratio, similarly to channel load, but apply it

to a subset of nodes, and queue length for another set of nodes. The node activates channel monitoring only when it receives a packet to forward. Therefore, there is no overhead to measure channel loading.

4.3 Channel Busyness Ratio and Throughput Measurement

Throughput is addition to channel busyness to take into account the effects of hidden nodes problem in multi-hop environment. The throughput quantifies the number of successful transmissions.

Packet service time: The inverse of packet service rate, it is the interval between packet arrival at the MAC layer and its successful transmission. It covers packet waiting, collision resolution, and packet transmission time at the MAC layer.

The congestion control cannot be decoupled from the MAC protocol, and adequate protocol should first be used to avoid congestion. In applications where the event cannot be known a priory, random access contention based MAC protocols are necessary (CSMA "Carrier Sense Multiple Access"-based). Continuous periodic applications with high rate a TDMA "Time Division Multiple Access"-like scheme is more appropriate.

V. RESULTS AND DISCUSSION

5.1 EXPERIMENTAL SETUP

Congestion in a network may occur if the load on the network the number of packets sent to the network is greater than the capacity of the network the number of packets a network can handle. Congestion control refers to the mechanisms and techniques to control the congestion. The congestion control having a different type of models but it have some disadvantage .To overcome the drawbacks, we proposed evolutionary algorithm, ant colony algorithm to get the optimal solution for the congestion control. In order to avoid congestion delays, the ant colony optimization paradigm is explored to find a optimize routes and to proposed routing algorithms are simple yet efficient. The routing optimization is driven by the minimization of total latency during packets transmission between the tasks.

5.2 DYNAMIC SOURCE ROUTING (DSR)

Genetic algorithms are a part of evolutionary computing. It is also an efficient search method that has been used for path selection in networks. These stochastic search algorithms are based on the principle of natural selection and recombination. GA has been an efficient search method based on principles of natural selection and genetics. They are being applied successfully to find acceptable solutions to problems in business, engineering, and science.

We can find good solution for adequate amount of data at hand, but the complexity of data increases as GA takes time to find the solution. GA works well for network model to find the optimal path. In this, the source and the destination nodes are sure to participate in every generation. Other nodes or the genes become a part of the chromosome if they find an optimal path between the source and destination. GA is composed with a set of solutions, which represents the chromosomes. This composed set is referred to population. Population consists of set of chromosome which is assumed to give solutions. From this population, we randomly choose the first generation from which solutions are obtained. These solutions become a part of the next generation. Within the population, the chromosomes are tested to see whether they give a valid solution. This testing operation is nothing but the fitness functions which are applied on the chromosome. Operations like selection, crossover and mutation are applied on the selected chromosome to obtain the progeny. Again fitness function is applied to these progeny to test for its fitness. Most fit progeny chromosome will be the participants in the next generation. The disadvantage of this protocol is that the route maintenance

mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in GAs. This routing overhead is directly proportional to the path length.

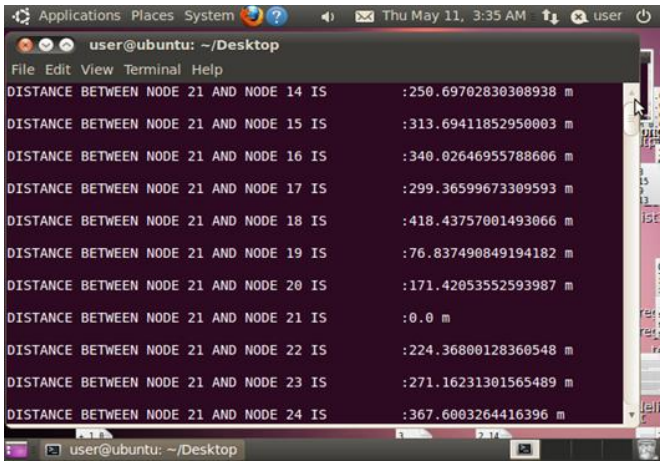

Figure-3: Calculate the Distance between all the Nodes

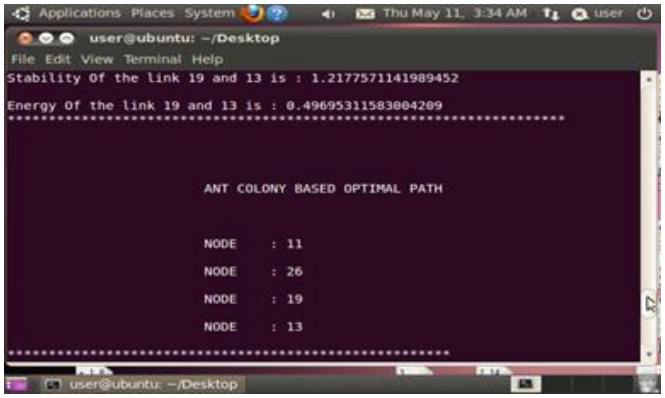

Figure-4: After the Selection of Source and Destination Calculate the Distance between their Neighbouring Nodes

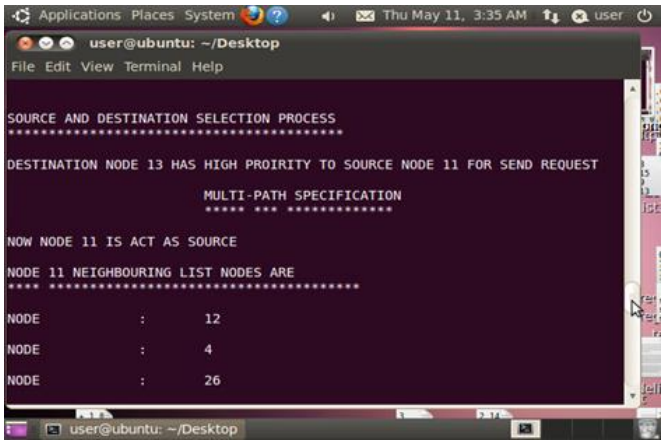

Figure-5: List out the Neighbouring Node

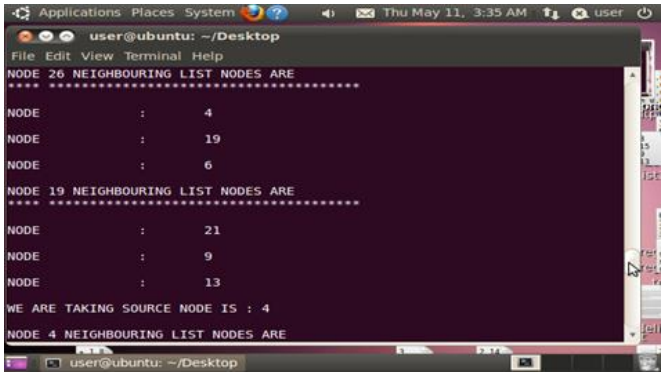

Figure-6: Finally Display the Optimal Path between Source and Destionation

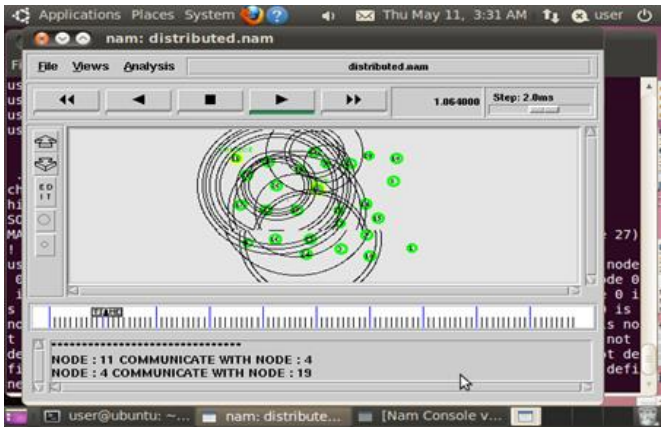

Figure-7: Neighbouring Path between the Source and Destination

VI. CONCLUSION

I propose distributed IDS for CRNs based on evidence theory. Aim to get more accurate final detection result making at CDC, we apply D-S theory of evidence to combine different detection data and credibility from every IDS Agents. Simulations presented show that the proposed system performs more excellent than the traditional Weighted Fair Queuing (WFQ) Combination algorithm.

VII. FUTURE ENHANCEMENT

In my future work, I would like to work on any cast routing protocols to check the efficiency under high throughput applications, e.g. multimedia applications by employing negotiation parameters in route request packet in finding nearest server through non congestion paths.

VIII. REFERENCES

[1]. T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.

[2]. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[3]. A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks, "Computer Comm.,vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.

[4]. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks," IEEE Trans. Wireless Comm.,vol. 1, no. 4, pp. 660-670, Oct. 2002.

[5]. A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[6]. S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks, "Computer Comm.,vol. 30, nos. 14/15, pp. 2842-2852, 2007.

[7]. K. Pradeepa,W.R.Anne, andS.Duraisamy,"Design and Implementation Issues of Clustering in Wireless Sensor Net-works," Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.

[8]. L.B. Oliveira et al., "Sec LEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.

[9]. K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM),pp. 1-5, 2008.

[10]. P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA),pp. 145-152, 2007.

[11]. K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM),pp. 1-5, 2008.