International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 4, Issue 3
March 2016.
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395

Received on: 28.2.2016 Published on: 14.3.2016 Pages : 4 - 12

TRUST BASED ROUTING IN WIRELESS SENSOR NETWORK

Mr.S.Ohm shankar [a*],Mrs. D. Maheswari [b*] ,

Department of Electronics and Communication Engineering, Agni college of Technology. Chennai 600130 Tamil nadu India
a e-mail: ohmshankar.ece@act.edu.in, b e-mail: maheswarid.ece@act.edu.in

ABSTRACT

A Sensor Node deployed in the Wireless sensor network (WSN) has the capability to read the sensed information and transmit or forward information to base stations or a sink node through multi-hop routing. In WSN nodes may be compromised and perform malicious attacks such as packet dropping or packet modifications to disrupt normal operations of a WSN wherein Sensor Nodes usually perform unattended operations. I propose a hierarchical trust management protocol leveraging clustering to cope with a large number of heterogeneous SNs for scalability and reconfigurability, as well as to cope with selfish or malicious SNs for survivability and intrusion tolerance. I propose a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two aspects of trust worthiness, namely, social trust and QoS trust. Social trust refers to properties derived from social relationships. Some metrics to measure these social trust properties can be frequency of communication, and quality of reputation. Second, QoS trust represents competence, dependability, reliability, successful experience. This provides reliable communication in WSN

1.0 Introduction

The Trust based protocols in wireless sensor network to improve the reliability. Due to the increasing popularity of wireless networks, there is an increasing need for security. This is because unlike wired networks, wireless networks can be easily hacked from outside of your building unless the proper security measures are in place. This Project examines the various issues regarding wireless security and the methods you can employ to safeguard the wireless network. Any node under attack in ad hoc network exhibits an anomalous behaviour called the malicious behaviour. In this situation, the entire operation of a network gets disturbed and to preclude such malicious behaviour several security solutions have been discovered. In this Project, malicious behaviour of a node is defined and to defend such behaviour, security solutions are presented which are used in furnishing a secure and reliable communication in ad hoc.

Mobile ad hoc network (MANET) is a dynamic wireless network with or without fixed infrastructure. Nodes may move freely and organize themselves arbitrarily. Sparse MANETs are a class of ad hoc networks in which the node population is sparse, and the contacts between the nodes in the network are infrequent.

Traditional MANET routing protocols such as AODV, DSDV and LAR make the assumption that the network graph is fully connected and fail to route messages if there is not a complete route from source to destination at the time of sending. One solution to overcome this issue is to exploit node mobility in order to

carry messages physically between disconnected parts of the network. These schemes are sometimes referred to as mobility-assisted routing that employ the store-carry-and-forward model.

Mobility-assisted routing consists of each node independently making forwarding decisions that take place when two nodes meet. A message gets forwarded to encountered nodes until it reaches its destination. Current research supports the observation that encounters between nodes in real environments do not occur randomly and that nodes do not have an equal probability of encountering a set of nodes. As a consequence, not all nodes are equally likely to encounter each other, and nodes need to assess the probability that they will encounter the destination node. An analysis on real-world encounters based on network traffic traces of different university campus wireless networks. Their analysis found that node encounters are sufficient to build a connected relationship graph, which is a small-world graph. Therefore, social analysis techniques are promising for estimating the social structure of node encounters in a number of classes of disconnected delay-tolerant MANETs (DDTMs).

Social networks exhibit the small-world phenomenon, which comes from the observation that individuals are often linked by a short chain of acquaintances. The classic example is Milgrams 1967 experiment [3], where 60 letters were sent to various people located in Nebraska to be delivered to a stockbroker located in Boston. The letters could only be forwarded to someone whom the current letter holder knew by first name and who was assumed to be more likely than the current holder to know the person to whom the letters were addressed. The results showed that the median chain length of intermediate letter holders was approximately 6, giving rise to the notion of "six degrees of separation." Milgram's experiment [3] showed that the characteristic path length in the real world can be short. Of particular interest, however, is that the participants did not send on the letters to the next participant randomly but sent the letter to a person they perceived might be a good carrier for the message based on their own local information. In order to harness the benefits of small-world networks for the purposes of message delivery, a mechanism for intelligently selecting good carriers based on local information must be explored.

The objective of this project is creating nodes in an ordered way and transforming or forwarding information through the shortest path. A node which is not forwarding the packets is called malicious node. Detection of malicious node is the task of this project. Problem arises due to this malicious node solved in the second phase of this project.

II SURVEY OF WSN

A Significance

A wireless sensor network (WSN) consists of autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

In this project, a new trust based wireless protocol used to improve the performance of the sensor node and reliability. Simulation experiments were used to study the design trade-offs between the proposed and existing method in terms of reliability issues.

Group-based trust management scheme for clustered WSNs in which each SN performs peer evaluation based on direct observations or recommendations, and each cluster head (CH) evaluates other CHs as well as SNs under its own cluster. This work is similar to the hierarchical structure is employed for scalability. However, trust in their case is assessed only based on past interaction experiences in message delivery, which in this case is just one possible trust component along with other social and QoS trust components comprising the overall trust metric. Furthermore, trust formation issue (i.e., how a peer-to-peer trust value is formed) to maximize application performance.

They also considered a decay function that captures the changing nature of trust in trust calculations. However, their work is theoretical in nature without addressing what trust attributes should be used (a trust composition issue), how trust is aggregated accurately (a trust aggregation issue), or what weights should be put on trust attributes to form trust (a trust formation issue). On the contrary, this work addresses all three aspects of trust management. Moreover, address protocol validation issues by devising a mathematical model yielding objective trust against which subjective trust from protocol execution may be compared for assessing its accuracy.

Intrusion detection is the last defence to cope with malicious nodes for WSNs in which SNs can be compromised due to capture or virus infection. Existing work was mostly based on anomaly detection techniques to discover deviations from expected behaviours, including rule-based weighted summation data clustering and Support Vector Machine (SVM) In rule-based anomaly detection typically rules based on QoS metrics are being setup to detect suspected attack behaviours, e.g., if a SN does not forward a packet within a time limit, if a SN forwards the same packet multiple times without suppression, or if a packet is received directly from a non-neighbour SN or from a neighbour SN who is not supposed to send a packet during a particular time interval, then the SN in question is suspected of maliciousness.

When a SN's "maliciousness count" exceeds a tolerance limit, the SN is diagnosed as compromised. The main drawback of rule-based anomaly detection is that it cannot cope with anomalies not covered by rules, thus leading to high false negatives when unknown anomalies appear. In the weighted summation approach each SN has a weight associated with it representing the trustworthiness of its sensor reading output. The system periodically calculates the average sensor reading output by taking a weighted summation out of all sensor reading outputs. The weight associated with a SN is dynamically updated according to the deviation of the SN's output from the average output. A larger deviation results in a lower weight. Once the weight of a SN falls below a threshold, the SN is considered a malicious node. The main drawback of this approach is a high false positive probability may result. In the clustering based approach, SNs reporting similar sensor reading data out of selected data features are clustered together.

Consequently, a SN that does not belong to any cluster or belong to a small cluster is considered an outlier or a compromised SN. The effectiveness of this approach hinges on the accuracy of the underlying clustering algorithm achievable only through heavy learning and computation which may impede its use for real time operation. In SVM-based anomaly detection, a kernel function is chosen to map the input data space into a higher dimensional space. The anomaly detection is formulated as a quadratic optimization problem to find a minimum hyper sphere that includes the majority of the data points with a certain degree of similarity. The data points that are outside of this hyper-sphere are considered anomalies. However, the challenge of using SVM-based intrusion detection in WSNs is the computational complexity of solving the optimization problem, thus preventing its use for real time operation. A general problem with anomaly detection is high false alarms because noises in wireless transmission may cause uncertainty of information, and limited resources may cause inability to collect accurate and needed information. In this Project, trust-based intrusion detection and compare its performance with weighted summation and data clustering anomaly detection techniques. Trust-based intrusion detection has received much attention in the literature because of its elasticity against uncertainty and resiliency against attacks.

They employed the concepts of evidence chain and trust fluctuation to evaluate a node in the network, with the evidence chain detecting misbehaviours of a node, and the trust fluctuation reflecting the high variability of a node's trust value over a time window. They split the reputation information into trust and confidence for reputation exchanges and then combine them into trustworthiness for intrusion detection. Trust evaluation as a path problem and used path semi ring and distance semi ring operators to combine opinions such that two nodes can establish an indirect trust relation without previous direct interactions. Most trust-based intrusion detection mechanisms employed for MANETs cannot be directly implemented in WSNs due to limited battery power and resources in SNs. In this Project, hierarchical trust management leveraging clustering to implement light-weight trust-based intrusion detection for WSNs.

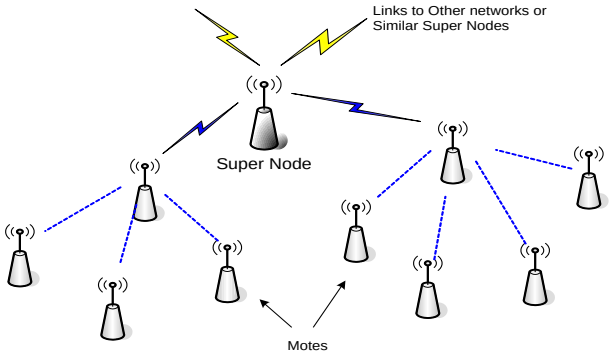


Fig 1.1 Structure of nodes.

Hierarchical trust management for WSNs and its application to trust-based routing and which considered its application to trust-based intrusion detection. The protocol design is extended with new design concepts of trust aggregation protocol accuracy i.e., identifying and validating the best trust aggregation and propagation protocol setting for each individual trust property such that subjective trust obtained as a result of protocol execution is close to objective trust or ground truth.

Dynamic trust management, i.e., identifying and validating the best way to form trust out of QoS and social trust properties dynamically (in terms of the best weights used for trust properties) in response to changing conditions such as increasing hostility to maximize application performance; and application-level trust optimization, i.e., identifying the best way to use trust for application performance optimization. Both applications have been substantially extended to demonstrate the feasibility of these new design concepts.

APPLICATIONS OF WSN

Because most of the knowledge of sensor networks is basic on the application at the beginning, especially two important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SenIT) form the defense Advanced Research Project Agency (DARPA), sensor networks are applied very successfully in the military sensing. Now wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance reconnaissance and targeting systems. In the battlefield context, rapid deployment, self-organization, fault tolerance security of the network should be required. The sensor devices or nodes should provide following services: Monitoring friendly forces, equipment and ammunition Battlefield surveillance, Reconnaissance of opposing forces Targeting, Battle damage assessment Nuclear, biological and chemical attack detection reconnaissance.

In Environmental applications includes sensor networks are also widely applied in habitat monitoring, agriculture research, fire detection and traffic control. Because there is no interruption to the environment, sensor networks in environmental area is not that strict as in battlefield. Bush fire response, A low cost distributed sensor network for environmental monitor and disaster response. An integrated network of sensors combining on the ground sensors monitoring local moisture levels, humidity wind speed direction, together with satellite imaginary and longer term meteorological forecasting will enable the determination of fire risk levels in targeted regions.

SYSTEM ANALYSIS

A sensor node (SN) deployed in the WSN has the capability to read the sensed information and transmit or forward information to base stations or a sink node through multi-hop routing. Sensors have severely restricted resources such as energy, memory, and computational power.

A more serious issue is that nodes may be compromised and perform malicious attacks such as packet dropping or packet modifications to disrupt normal operations of a WSN.SNs usually perform unattended operations. A large number of SNs deployed in the WSN also require a scalable algorithm for highly reconfigurable communication operations.

Cluster-based WSN consisting of multiple clusters, each with a cluster head and a number of SNs in the corresponding geographical area. CH nodes have more power and resources than SN nodes. The CH in each cluster may be selected based on an election protocol such as HEED at runtime to balance energy consumption versus Cluster Head functionality. A SN forwards its sensor reading to its Cluster Head through SNs in the same cluster and the CH then forwards the data to the base station or the destination node through other Cluster Head.

Leveraging this two-level of hierarchy in the WSN, trust management protocol is conducted using periodic peer-to-peer trust evaluation between two SNs and between two Cluster Heads. At the SN level, each SN is responsible to report its peer-toper trust evaluation results towards other SNs in the same cluster to its CH which performs CH-to-SN trust evaluation towards all SNs in its cluster. Similarly a CH is responsible to report its peer-to-peer trust evaluation results towards other CHs in the system to the base station which performs station to-CH trust evaluation towards all CHs in the system. The protocols for performing peer to- peer, CH-to-SN and station-to-CH trust evaluations. It compose trust metric by considering both social trust and QoS trust to take into account the effect of both aspects of trust on trustworthiness. Social trust in the context of wireless sensors may include intimacy, honesty, privacy, centrality, and connectivity. QoS trust may include competence, cooperativeness, reliability, task completion capability, etc. Trust protocol such that it is generic and can take a combination of social trust and QoS trust metrics to form the overall trust metric without loss of generality.

In this work they consider intimacy and honesty measure social trust derived from social networks. Selection of energy and unselfishness to measure QoS trust derived from communication networks. The intimacy trust component reflects the relative degree of interaction experiences between two nodes. It follows the maturity model proposed in that the more positive experiences SN A had with SN B, the more trust and confidence SN A will have toward SN B. The honesty trust component strongly implies whether a node is malicious or not.

The assumption is that a compromised node is malicious in nature and thus dishonest. Energy is an important metric in WSNs since SNs are extremely constrained in energy. It uses energy as a QoS trust metric to measure if a SN is competent in performing its intended function. The unselfishness trust component reflects if a SN can cooperatively execute the intended protocol. Trust management protocol can apply to any WSN consisting of heterogeneous SNs with vastly different initial energy levels and different degrees of malicious or selfish behaviours. A SN is more likely to become selfish when it has low energy or it has many unselfish neighbour nodes around. Further, a SN is more likely to become compromised when it has more compromised neighbours around. A CH consumes more energy than SNs. After a SN or CH is compromised, it may consume even more energy to perform attacks.

B PROPOSED SYSTEM

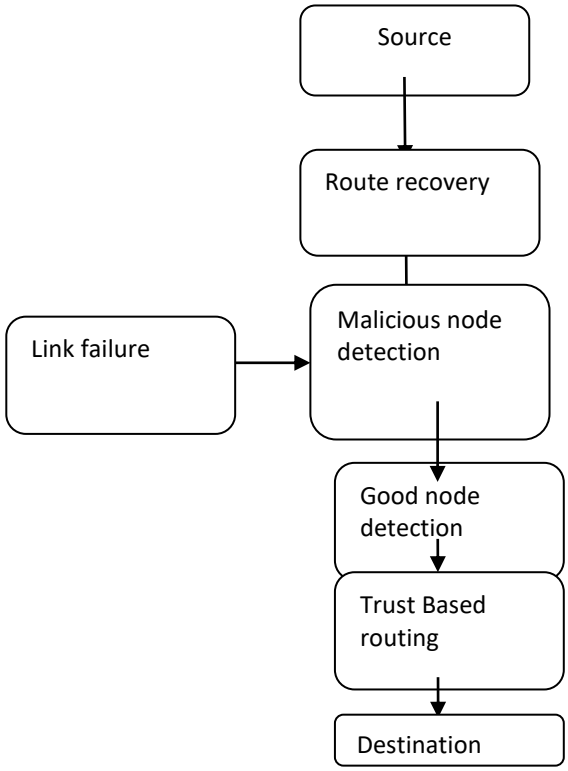
A hierarchical dynamic trust management protocol is proposed for cluster-based WSN, considering two aspects of trust worthiness they are, social trust and QoS trust. A probability model is proposed utilizing stochastic Petri nets techniques to analyze the protocol performance and validated subjective trust against objective trust being obtained based on ground truth node status. Feasibility of dynamic hierarchical trust management and application-level trust optimization design concepts with trust-based geographic routing and trust-based IDS applications.

A new distributed approach that establishes reputation-based trust among sensor nodes in order to identify malfunctioning and malicious sensor nodes and minimize their impact on applications. This method adapts well to the special characteristics of wireless sensor networks, the most important being their resource limitations.

This methodology computes statistical trust and a confidence interval around the trust based on direct and indirect experiences of sensor node behavior. By considering the trust confidence interval, the tradeoff between the tightness of the trust confidence interval with the resources used in collecting experiences. Furthermore, this approach allows dynamic scaling of redundancy levels based on the trust relationship between the nodes of a wireless sensor network. Using extensive simulations demonstrate the benefits of this approach over an approach that uses static redundancy levels in terms of reduced energy consumption and longer life of the network. High
confidence trust can be computed on each node with a relatively small memory overhead and used to determine the level of redundancy operations among nodes in the system.

Sensor networks are distributed networks made up of small sensing devices equipped with processors, memory, and short-range wireless communication. They differ from traditional computer networks in that they have resource constraints, unbalanced mixture traffic, data redundancy, network dynamics, and energy balance. Work within wireless sensor networks (WSNs) Quality of service (QoS) has been isolated and specific either on certain functional layers or application scenarios. However the area of sensor network quality of service (QoS) remains largely open. In this project WSNs QoS requirements within a WSNs application, and then analyzing Issues for QoS Monitoring.

IV BLOCK DIAGRAM



Communication networks significantly increase the processing capacities of computers. Distributed applications, like FTP (File Transfer Protocol), are being used in the administrations of most companies. The main requirement of these applications is that they must be reliable. As a consequence, computer networks must offer the highest QOS. To achieve and to maintain the required QOS, the network's managers must attend to the performance of the communication system. Three general approaches to evaluate the performances of a system are identified:

1. Measurement tools
2. Analytical techniques
3. Simulation techniques

Measurement tools consists of evaluating directly the network behaviour, with the help of measurement tools or monitors . These tools support the activities of data collection, data reduction, and statistical analysis. This technique is not performed on the real-system but on a model of the system. They are often called performance prediction techniques, as they reveal the performance of a new and non-operational system. Analytical techniques employ a system of equations; the mathematical resolution of these equations yields exact quantitative results.

Simulation consists to use a computer to evaluate a model numerically, and data are gathered to estimate the desired true characteristics of the model. The analytical techniques cover a very narrow range of utilization. As the model must stay simple, many details of the system are neglected and it becomes no realistic. Simulation allows to deal with a complex model. In communication networks, the models are often complex and require a long and tedious task owing to the size, diversity and complexity of communication systems. To set a new configuration or to detect design errors early, the network manager or system designer need tools for

performance prediction that bring them an assistance in the way to master the complexity of his/her task. These tools are based upon the discrete event simulation.

- OPNET
- GLOMOSIM
- QUALNET
- OMNET ++
- NETSIM

Network simulation soft network communication design is an important step and it is also the key to network communication performance analysis.
Then it analyses the system structure, NS2 method and simulation design process. And finally it conducts an experiment on the Distiller's tail queue algorithm by NS2 and gets useful data to prove the validity of the simulation and obtains the generic methods of network communication.

Front End: TCL (Tool Command Language)
Back End: C++
Network Simulator-2

c MOTIVATION FOR SIMULATIONS

- Cheap does not require costly equipment
- Complex scenarios can be easily tested
- Results can be quickly obtained – more ideas can be tested in a smaller timeframe
- The real thing isn't yet available
- Controlled experimental conditions Repeatability helps aid debugging

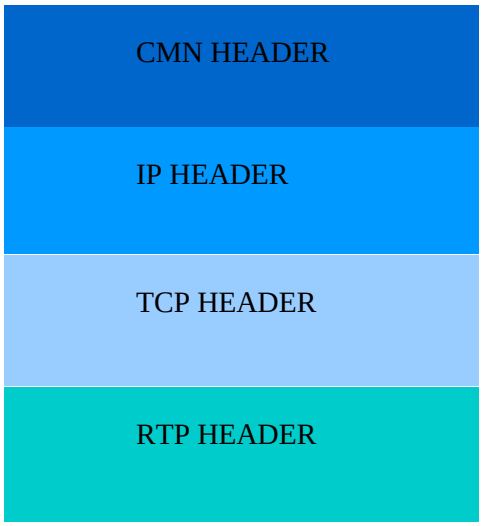
NS is an object oriented discrete event simulator. Simulator maintains of list events and executes one event after another. Single thread of control, no locking or race conditions.

NS programming structure is

- Create the event scheduler
  - Turn on tracing
  - Create network topology
  - Create transport connections

In this Event scheduler while processing many data at a time it will process one by one FIFO concept , so there is no congestion while transferring the packets.

It is the collection of data, whether header is called or not all header files where present in the stack registers.



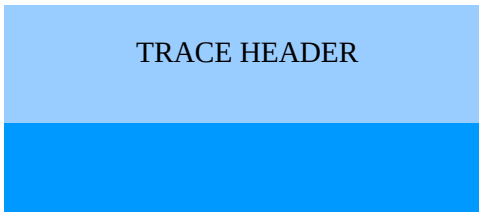


Fig : 4.6.1 Stack registers

SIMULATION RESULTS

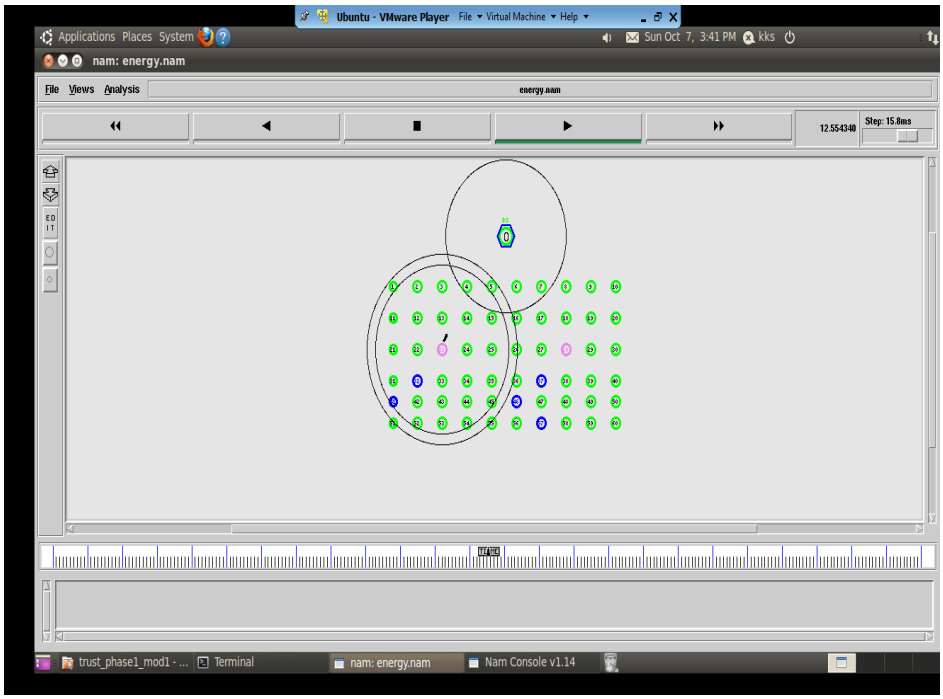
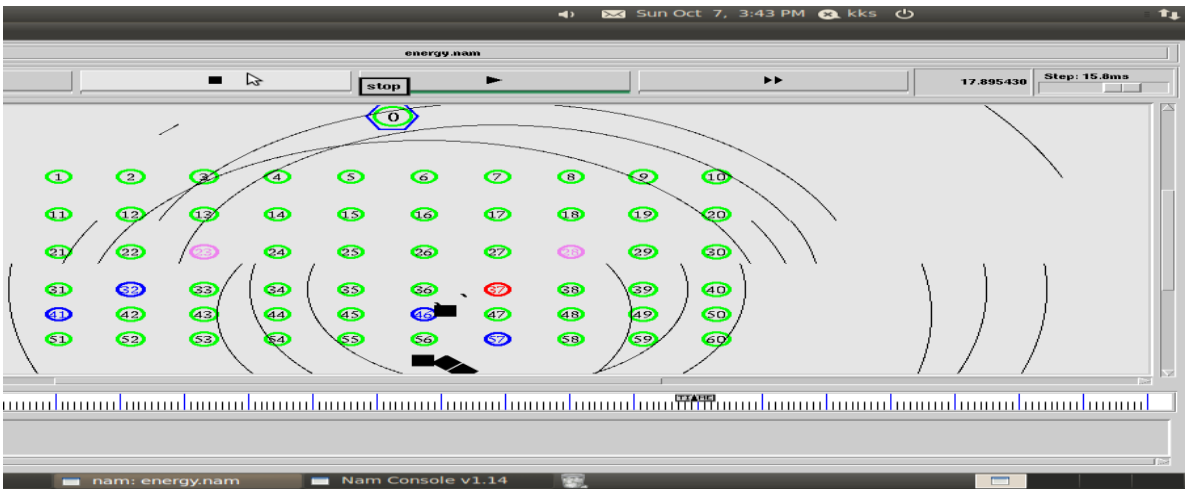


Fig 6.1 Route selection output



V CONCLUSION

Thus the proposed model provides much reliability in the transferring of data packets to the base stations. Here shortest route is selected by the nodes. This Project examines the various issues regarding wireless security and the methods you can employ to safeguard the wireless network. Any node under attack in ad hoc network exhibits an anomalous behaviour called the malicious behaviour. In this situation, the entire operation of a network gets disturbed and to preclude such malicious behaviour several security solutions have been discovered. In this Project, malicious behaviour of a node is defined and to defend such behaviour, security solutions are presented which are used in furnishing a secure and reliable communication in ad hoc. During the processing, some nodes act as a malicious node, which does not forward packets to the other nodes. It resends the packets back to the sender. In this module we are identifying the malicious node.

In module 2, problems occurs due to malicious nodes will be recovered which helps to forward the packets to base station without any interruption.

References:

1. OssaiiiaYounis and Sonia Fahmy "Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 6, pp. 721-734, June 2008.
2. Pon.R, M.A. Batalin, J. Gordon, A. Kansal, D. Liu, M. Rahimi, L.Shirachi, Y. Yu, M. Hansen, W.J. Kaiser, M. Srivastava, G.Sukhatme, and D. Estrin, "Networked Infomechanical Systems: A Mobile Embedded Networked Sensor Platform," Proc. ACM/IEEE Int'l Symp. In