Geocentric Based Node Detection and Revoking Malicious Node in WSN

Karthik. V[1], Ms. Karthikayini[2], Dr S Mohan Kumar[3], Ms. Gayathri.T[4]
[1, 2, 3, 4] Department of CSE
[1, 2, 3, 4] New Horizon College of Engineering, Bangalore, Karnataka, India

Abstract- *A location based routing is a aggregation of mobile nodes that are dynamic and arbitrarily located in such a way that the interconnections between nodes are capable of changing on a continual base. The main destination of this routing is correct and efficient route establishment between a couple of guests so that messages may be presented in a timely fashion. Terminode routing aims to support location-based routing on irregular topologies with mobile nodes. It accomplishes its goal by combining a location-based routing method with a link state-established mechanism. Farther, it brings in the concept of anchors, which are geographical points, imagined by sources for routing to specific goals, and proposes low overhead methods for computing anchors. Concluding, a special sort of restricted search mode (Restricted Local Flooding, RLF), solves problems due to the inaccuracy of location information, in particular for control packets. The performance analysis indicates that, in large mobile ad hoc networks, terminode routing performs better than MANET-like, or existing location-based routing protocols. It does so by keeping up its routing overhead low and by efficiently solving location inaccuracies.*

Keywords- DSR (Dynamic Source Routing), GPS (Global Positioning System), adhoc networks, Sensor Networks, Wireless Sensor Network(WSN), Malicious Beacon Nodes, Network Topology, Dynamic Mobility, Localization, On-Demand Multicast Routing Protocol (ODMRP), Mobile Ad Hoc Networks (MANETs).

I. INTRODUCTION

A location based routing is a aggregation of mobile nodes that are dynamic and arbitrarily located in such a way that the interconnections between nodes are capable of changing on a continual base. The main destination of this routing is correct and efficient route establishment between a couple of guests so that messages may be presented in a timely fashion. LAR is an on-demand protocol who is based on the DSR (Dynamic Source Routing). The Location Aided Routing protocol uses location data to reduce routing overhead of the ad-hoc network! Normally the LAR protocol uses the GPS (Global Positioning System) to get these location information. With the availability of GPS, the mobile hosts know their physical position.

Unlike traditional distance networks, networks do not bank on any fixed infrastructure. Alternatively, hosts rely on each other to maintain the network plugged into. The military tactical and other security-sensitive operations are however the primary applications of ad hoc networks, although there is a tendency to take on ad hoc networks for commercial purposes due to their unique properties. One primary challenge in the invention of these nets is their exposure to security attacks. In this report, we examine the threats an ad hoc network faces and the security goals to be accomplished. We identify the new challenges and opportunities presented by this new networking environment and explore fresh approaches to secure its communication. In particular, we take advantage of the inherent redundancy in adhoc networks, multiple routes between nodes to defend routing against denial of service attempts. We also use replication and new cryptographic systems, such as threshold cryptography, to build a highly dependable and highly available key management service, which forms the heart of our security framework.

The nets are a fresh paradigm of wireless communication for mobile hosts (which we call nodes). In this routing, there is no set up infrastructure such as base stations or mobile switching centres. Mobile clients that pass along within each other's radio range directly via wireless connections, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology.

II. SURVEY WORK

A. DETECTING MALICIOUS BEACON NODES

Sensor locations play a vital function in many applications in sensor network. A routine of techniques has been proposed recently based on some extra clients to see the locations of regular sensors called beacon nodes, which are presumed to know their locations (e.g., by GPS receivers or configured manually). But, none of these techniques can operate in good order when there are malicious attempts,

particularly when some of the beacon nodes are compromised. This method presents a suite of techniques to detect and remove compromised beacon nodes that supply misleading location information to the regular sensors, targeting at providing secure location discovery services in wireless sensor nets.[1]. To detect malicious beacon signals these techniques start with an uncomplicated but effective method. To identify malicious beacon nodes and avoid false detection, this method also demonstrates various techniques to detect replayed beacon signals. (Donggang Liu et al., (2005)).

Secure distance-based location in the presence of cheating beacon nodes is an important problem in mobile wireless adhoc and sensor nets. Despite substantial research efforts in this way, some fundamental questions still remain unaddressed. When the act of cheating beacon nodes is larger than or equal to a given threshold, no two-dimensional distance-based localization algorithms exist that can guarantee a bounded error. In this method, the problem of robust space-based location in the presence of malicious beacon nodes will assume theoretically that the act of malicious beacon nodes is below threshold and derive a necessary and sufficient condition for having a bounded localization error and use heuristic algorithm that can achieve a bounded error. (M. K. Prakruthi et al., (2011)). The main goal here is to take a thorough analytical study of the space-based localization problem in the presence of cheating beacons. [3].

The nature of many applications using wireless sensor networks (WSNs) necessitates the use of security mechanisms. One of the primary issues in WSN is malicious nodes spoofing their identity and fix. In this method we(Atassi et al., (2013)) propose a decentralized malicious node detection technique based on the Received Signal Strength Indicator (RSSI). [5].

Routing in mobile ad hoc networks (MANETs) for groups should target at providing reliable and robust multicast routes to the group members against link and node failures with mobility conditions. T. Stephen John and A. Aranganathan in 2014 proposed this method, which offers an agent-based multicast routing scheme like On-Demand Multicast Routing Protocol (ODMRP) which can be more suitable for Ad Hoc network, only D-ODMRP Destination driven On-Demand Multicast Routing Protocol is utilized to shorten the number of nodes to be appended in the forwarding group. D-ODMRP introduces the characteristics into the existing on demand process of multicast forwarding structure in the MANET that builds a backbone in the frame of a reliable mesh and finds multicast routes. A mobile autonomous agent technique for intrusion detection system in MANET has been proposed where agents are discharged from a root node which traverses each node randomly and detect the malicious node. The link failure is noticed and repaired by nearby nodes. [6].

For many applications based on Mobile Ad Hoc Networks (MANETs), the location of the nodes is generally hard to be seen. In sensor networks, for example, such data may be vital for the MANETs. To boot, one problem to be fronted with this scenario is the fake parameters broadcasted by misbehaving/malicious nodes, which can either compromise results about positioning, or deplete power resources of mobile devices. Thus, in this method we(Silva et al., (2015)) propose a model for identifying the fake parameters broadcasted on the network, and for finding the malicious/misbehaving nodes. The Linear Regression and Variance Analysis (LRVA) are both the foundation for the multi-step-ahead predictions in this method. Through NS-2 and Aurora, we imitated the motion and energy expenditure of the nodes in a MANET, analyzing the time series of beacon-packets exchanged in the net. As a consequence of the LRVA employment, the fake parameters broadcasted in the network were detected, with the malicious/misbehaving nodes identified. The simulations presented in this method show low power use, which permits the joint employment of LRVA with other security techniques in the MANETs. [7].

The main challenge against deploying strong security algorithms is that WSNs suffer from major constraints in terms of power and computing resources. WSNs impose a primary condition on the design stage that requires any protocol or algorithm to be power-efficient. This stands for that strong cryptography techniques cannot be used and we need another layer of defense to protect the WSN. This makes intrusion detection systems (IDSs) an essential choice in these nets. IDSs can capture malicious misbehavior that makes out to get through the first layer of defense (i.e., cryptography and authentication). In this method we (M. Khanafer et al., (2016)) highlight the challenges met while planning an effective intrusion detection framework in WSNs, and offer a review of important contributions in this field. In conclusion, we offer a novel approach that helps in detecting and confining intrusive behavior in the web. [12].

Ad-hoc Networks are multi hop network in which there is no demand of central administration. Each and every node in Ad-hoc networks act as router to commit and get information. It stands for cooperation among the guests is significant for making communication between sender and corresponding receiver. [14]. It is not necessary that each node act as a cooperative node, some nodes can intentionally act as uncooperative or misbehavior nodes. Because of not taking in any trusted centralized authority in Ad-hoc network and

membership of nodes are constantly changing, detection of such misbehavior nodes is not thus comfortable. Ace of the effective technique to detect malicious nodes and isolate them from communication is CONFIDANT (Cooperation of Nodes Fairness in Dynamic Ad-hoc Network). Unluckily, this proficiency is also contained with some failings. This method proposed a malicious node detection technique, called Improved CONFIDANT technique which is inspired from CONFIDANT technique and resolves significant problems of CONFIDANT technique such as detection and prevention of Blackhole Nodes, false reporting problem, network collision as well as providing Quality of Service (QOS). (N. Devi and R. Sunitha (2016)).

B. LOCATION BASED NODE DETECTION

Vehicle-to-vehicle communication among vehicular ad hoc networks (VANETs) plays an important function in providing a high degree of safety and convenience for drivers. Geographic routing protocol has been identified to be suitable for VANETs because of the limited nature of such nets, e.g., frequently changed network topology and high dynamic mobility. (Z. Ren et al., (2009)). At that point is considerable functional research about geographic routing, but the node location security issues have not been vastly concentrated on so far. While selecting every hop, the functioning and security can be affected severely by false position because of the position information importance of geographic routing. Making use of directional antennas, we suggest a novel detection mechanism capable of recognizing nodes faking about their positions in beacon message. By breaking through which directional antenna beacon messages are received, ones' neighborhood can be easily separated into two groups. In increase, aggregated with the three malicious node detection rules, nodes can efficiently detect malicious nodes around them after exchanging neighbors grouping information with each others. [2].

In wireless sensor networks (WSNs), effective use of the nodes available energy is the main goal which most of the routing protocols seek to accomplish. In fact, clustering based routing protocols have gained vast approval due to its merit of less energy exhaustion. The expended energy by one cluster is split into two principal terms, namely, the expended energy in intra-cluster communication (Intra-term) and the dissipated energy from the Cluster Head (CH) to turn over to the Base Station (BS), (Inter-term). Without a doubt, reducing both terms would have a big impact on enhancing the network lifetime. As the topology control plays a essential part in balancing the energy of nodes, we use a Location based Topology Control (LTC) to oversee the performance of the active nodes through the sensing area. Hence the Intra term is minimized. Moreover, four multiple levels of clustering hierarchy (FL-LEACH) are used. Actually, FL-LEACH is an extended work for three layers clustering (TL-LEACH). Both of them are based on restricting the number of clients which can communicate right away with BS. This reduces and balances the Inter-term. Simulation results indicate that our suggested protocol is more efficient than other established protocols, such as LEACH and TL-LEACH. [17].

The node replica attack is known to be dangerous to wireless sensor networks (WSNs) because it enables the adversary to extend the damage throughout the network with very low price. To stop such attack, we propose a similar estimation based scheme with group deployment knowledge. Compared with prior works, our proposal provides additional functionality that prevents replica from generating false location claims. (Yang et al., (2016)).

Stochastic Point location (SPL) problem, in which a learning machine (LM) (entity, robot, algorithm, etc.) attempts to locate a certain peak in an interval, belongs to the field of Machine Learning. During the process, LM is interacting with a stochastic environment so that the information available is likely incorrect. In some conventional methods, the line is sampled into discrete periods and the authors mainly consider the relation between two neighboring nodes. So, there are plenty of places for improvement in public presentation. In this method, we elaborate the relation from two neighboring nodes to three adjacent nodes based on the classical random walk-based triple level algorithm (RWTA) and subsequently propose a universal algorithm. The philosophy rests in a freshly-introduced parameter θ, which is delineated as the radio of the correlation between adjacent nodes to the correlation between spaced nodes. It changes from nil to one, and particularly if $\theta = 1$, the algorithm could be exactly evolved into "RWTA". For the reason that the whole scheme could be seen as the Markov chain, its transform diagram and transform matrix are construed, followed by a rigorous mathematical proof procedure of the overlap. It can be calculated that the proposed algorithm produces a larger stably convergent interval with $p > 0.236$ if $\theta = 0$, extending far beyond either Oommen's algorithm with $p > 0.5$ or RWTA with $p > 0.333$. [19].

This method offers a location-aided flooding mechanism to distribute data in community-based IoT networks. Prompted by two heuristics obtained from the psychoanalysis of the optimal flooding problem, the proposed mechanism allows wireless nodes to delete a duplicate packet transmission in a distributed way when all of their neighbors have got that packet in advance. Extensive evaluations have been made out in two different scenarios, i.e., a random

uniform distribution of wireless nodes and a real distribution of wireless clients in the Sumida ward of Tokyo. It has been validated that the suggested mechanism is not only capable to increase the success ratio of data delivery, but also capable of thinning out the delay of data delivery significantly. E.g., in the best case, the proposed mechanism improves the success ratio of conventional mechanisms by 47.3% and cuts the delivery delay by 92.0%. (W. Liu et al., (2017)).

C. WORMHOLE ATTACK

R. Jaiswal and S. Sharma in 2012 proposed a routing protocol called AOMDV. Dynamic topology and without infrastructure provide a big facility for Adhoc network. In such facility packet dropping is a severe challenge for quality performance of Adhoc network. Adhoc network suffered some security attack such attacks are wormhole attack, black hole attack, and malicious attack that attack took place a packet dropping problem in Adhoc network. For the minimization of attack and packet dropping various authors built various method such method is node authentication, passive feedback scheme, Acknowledgment based scheme, certification based scheme and incentive based scheme, certificate-based scheme suffered a problem of huge operating cost due to extra authentication packet. In this method we have used entropy of the nodes to realize whether it is abnormal node. To evaluate the randomness of any node we have used Reference-Broadcast Synchronization, a system in which nodes send reference beacons to their neighbors using physical-layer broadcasts. The proposed system for detecting warm hole node is implemented in NS2 and result shows the result of the warm hole attack on the normal behavior and, the improvement of functioning after the application of the proposed system. The rating of functioning is measured by the packet delivery ratio, normalized load, packet throughputs. In this dissertation, we used AOMDV as routing protocol. [4]. The figure 1 shows the path discovery.

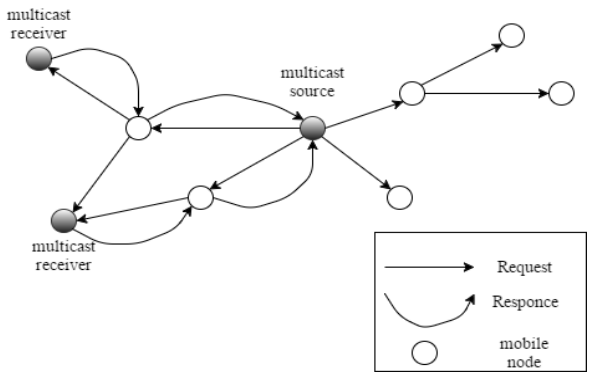

Figure 1. AOMDV path finding.

Challenges in meeting the best security standards are yet an unresolved question in the field of the mobile adhoc network, particularly pertaining to wormhole attack. Although in that respect are many existing solutions, but majority of them suffers from various trade-offs. This method discusses about the important issues of the existing techniques and gives a novel secure routing protocol that was found to have sufficient supportability of complex cryptographic algorithms as a security measure along with enhancement of data transmission operations. The proposed routing scheme is designed by enhancing the multicast routing protocols by adding few simple entities, e.g. Additional Supportive Beacons (ASR), Route-Discovery Beacons (RDB), and Auxiliary Nodes (AN). [8].

Wireless sensor networks have recently been widely read and utilized in long-term mission-critical environments, where reliable delivery of sensing information under multiple node failure is involved. In this work, we discuss tabu-list-based multi-path routing, which assures that multiple copies of the events are delivered through completely different paths, without requiring additional communications to exchange route information. Toward development of attack-tolerant multipath routing, we also look into the effects of wormhole attacks and location-aware wormhole detection scheme. [9].

Security of different networks has forever been a main concern as its necessary to protect the resources being shared and communication being done among the lawful users. If we let down our safeguards, an attacker can transform the routing protocol and interrupt the network operations through mechanisms such as packet drops, flooding, data fabrication, etc. MANET is a type of network whose dynamic topology, decentralizing governance and other such features are forever in favor of many security attacks. [10].

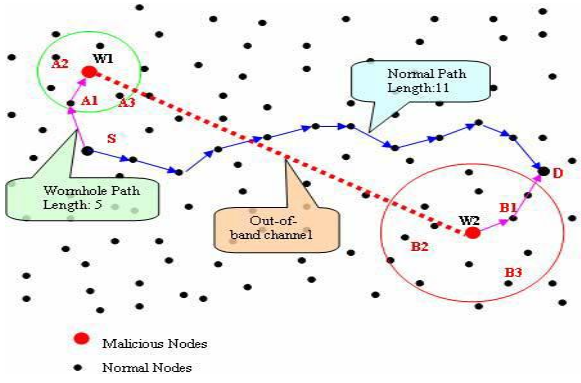

Figure 2. wormhole attack

Wireless Sensor Networks (WSNs) are utilized by IoT to collect, exchange, and deliver data remotely leveraging the potential of its in practical applications and helps. Yet,

delivering data remotely might be menaced by diverse and serious security attacks. This study concentrates on preparing a visual-aided tool for exposing security threats in IP-enabled WSNs. The proposed tool, called EyeSim, is a human interactive visual-based anomaly detection system that is capable of monitoring and promptly alerting to the presence of wormhole links. In summation, it is capable of indicating the malicious nodes that form the wormhole nexus. EyeSim may expose adversaries by conducting cognitive network data analysis based on dynamic routing information. The efficacy of EyeSim is assessed in terms of detection accuracy. The simulation results show that EyeSim has the capabilities to accurately detect multiple wormhole attacks in real-time. (N. Tsitsiroudi et al., (2016)).

A wireless sensor network (WSN) consists of a large number of sensor nodes with limited batteries, the sensing devices are deployed randomly on a zone to gather data. WSNs are threatened by several malicious behaviors caused by some guests. The shock of such behaviors can be severe, yet fatal, due to the collaborative nature of nodes in a network without fixed infrastructure. And so, in this study we have adverted to the demand for a secure network communication network with mechanisms that hold into account the special imaginations of the nodes. In lodge to accomplish such a surety, the mesh can be split into sectors, and mobile agents (MAs) can be employed to reject traffic intruders caused by Wormhole attacks taking into account energy constraint. Wormhole attack is a denial of service attack launched by malicious nodes by creating a tunnel through which the packets are played back to malicious nodes disrupting the communication channel and corrupting network routing. In society to measure the functioning of our proposition, we have taken out several simulation tests using the SINALGO simulator. The results obtained show that our proposal extends the life of the web, in terms of energy use and the rate of packet delivery. [13].

Mobile adhoc networks (MANETs) have been suggested to support dynamic scenarios where no base exists. Each client in the mesh acts as a host as well as a router and, forwards traffic to other clients. MANETs can be put up quickly and at low cost in contrast to infrastructure networks which may be cabled or wireless. There is an increasing threat of attacks on the MANET Wormhole attack is one of the active internal attacks in which two or more attacker nodes tunnel the traffic from one position to another placement in the mesh. Wormhole attack is a very big security issue of mobile ad hoc network. That cannot be easily detected in which two malicious or attacker node joins together and make tunnels between them. The proposed technique discovers an alternative path to the object client. Because the shortest path can have the malicious attacker. The carrying out of the secure route discovery protocol is performed using NS2 and by adjustment of the AODV routing protocol. [15].

(Akila et al., in (2016)). The primary purpose of this method is to improve the wireless system recital. Though there are many safeties measure hinder its wide use in common. Besides the well-known pollution attacks, here is one more stern hazard, that of wormhole attacks, which weaken the recital increase of web coding. Because the fundamental uniqueness of network coding systems are diversified different from usual wireless networks, the blow of wormhole attacks and counter measure is unknown. In this method, we enumerate wormholes overwhelming destructive blow on network coding system recital throughout this test. We offer a small algorithm to sense wormholes and illustrate its rightness thoroughly. For the disseminated wireless network, we use DAWN, Distributed detection Algorithm against Wormhole in wireless Network coding systems, by discovering the transform of the surge direction of the novel packets caused by wormholes. We thoroughly prove that DAWN pledges a better inferior bound of unbeaten discovery speed. We achieve on the resistance of DAWN beside conspiracy attacks. We find that the heftiness depends on the compactness of the network node, and establish an essential place to attain collusion resistance. DAWN doesn’t rely on any spot sequence, global governance. It relies solely on local sequence which can attain usual network coding protocols, and the operating cost of the algorithm is moderate. [16].

III. EXISTING SYSTEM

A. Infra-structured Networks

The inaugural ace is to inaugurate a third fixed party (a base station) that will hand over the offered traffic from a station to another, as illustrated in Figure 3. The same entity will determine the attribution of radio resources, for example. When a node S wishes to pass on to a node D, the former notifies the home post, which eventually sets up a communication with the destination client. At this stage, the communicating nodes do not ask to know of a route from one to each other. All that matters is that both node's source and destination are within the transmitting range of the base station. If one of them fails to fulfil this condition, the communication will abort.

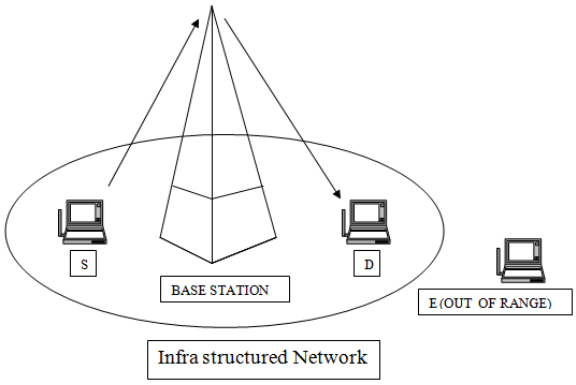

Figure 3. Infra structured Network

Here the base station's range is illustrated by the ellipse. The two nodes S and D which wants to communicate are in the scope of the base station. S send the message to the base station, which in turn forwards it to destination node D. This communication is carried out with the aid of a base station. All messages have to pass through the base station. Node E is out of the scope of the base station this prevents it from communicating with other clients in the mesh. When node E wants to transmit to any client in the network it has to contact the home post. Since it is out of range communication is not possible.

What occurs if the base station is unavailable? Or what goes on if we are in a place where such an infrastructure does not exist in the first position?

The answer is that we simply do not communicate! This is where the second approach is utilitarian. Note however that this kind of centralized administration is really popular among wide cellular networks such as GSM, etc.

B. Restrictions

The tracing are the limitations of the existing organization.

- Maintenance of information is performed manually
- Data aggregation is non uniform and is stored in different kinds
- Placing the appropriate host and customer profile and updating it whenever required becomes awkward.
- Enforcement of data integrity not possible.
- Unavailable of prominent security measures for information aggregation.

IV. PROPOSED SYSTEM

A. Location Based Routing

The concept behind these infra-structureless networks are the collaboration between its participating members, i.e., instead of taking in data transit through a specified base station, nodes consequentially forward data packets from one to another to a destination node is ultimately achieved. Typically, a packet may go through a number of network points before arriving at its address.

Location Based Routing introduces a totally new tone of network organization. The routers and hosts are free to act randomly and organize themselves in an arbitrary manner, hence the network topology changes rapidly and erratically. Absence of a backing structure in mobile ad-hoc networks, to a certain extent, invalidates almost all of the existing techniques developed for routine network controls in the existing wireless networks.

A MANET consists of mobile platforms (e.g., a router with multiple servers and wireless communications devices) --herein simply referred to as "nodes"--which are detached to move around at random.y. The lymph glands may be placed in or on airplanes, ships, trucks, cars, possibly even on people or very small devices, and there may be multiple hosts per router. A MANET is an independent organization of mobile clients. The organization may function in isolation, or may have gateways to and interface with a fixed mesh.

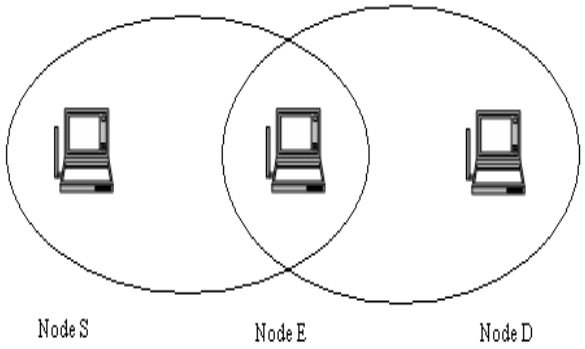

Figure 4. Infra-structure less Network

Here the node S wants to communicate to node D. The oval indicates the communication range of the client. The communication range of S does not exceed to include D. In this case routing is necessary, node E is in the range of S which has a D in its reach. So S in order to communicate with D, first sends the message to E which in turn forwards it to D. Thus the node E acts as a router and a node.

V. DATA FLOW DIAGRAM

The data flow diagrams are very helpful in determining the flow of data in an application.

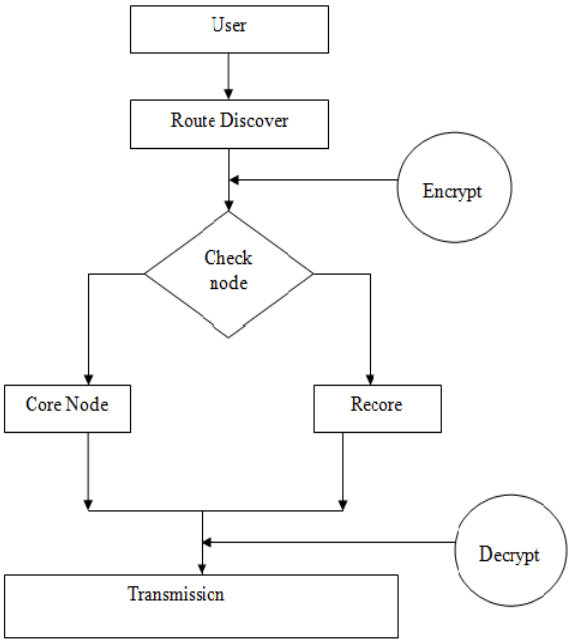

Figure 5.

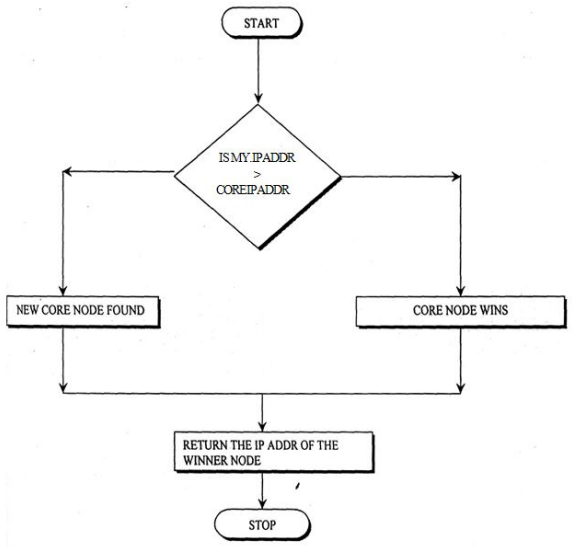

Figure 6.

VI. MODULES

- Expand Ring Search Algorithm
- Core Resolution Algorithm
- Tree Creation Algorithm
- Threshold Cryptography

Module Description

A. Expand Ring Search Algorithm

To initiate the Route Discovery, node transmits a "Route Request" as a single local broadcast packet, which is received by (approximately) all nodes currently on the transmission range of, including node. Each Route Request identifies the initiator and target of the Route Discovery, and also contains a unique request identification determined by the initiator of the Request. Each Route Request also contains a record listing the address of each intermediate node through which this particular copy of the Route Request has been forwarded.

B. Core Resolution Algorithm

Core Finding

- If the core node and user defined destination node are same then it transmits the file to the corresponding destination node.
- After route discovery, to find the core node of the system then compares core node and user defined node in core class
- Re-Core Selection
- To select the re-core node address for finding the destination address.
- Re-Core selection is used when the core process is not able to find the destination address.

C. Tree Creation Algorithm

When the intermediate node is fail, this process will execute and choose the another intermediate node for transmission. The failure node is identified by route request of corresponding end host, then the user to choose the another node as intermediate node so that the node failure will not affect the whole network

D. Threshold Cryptography

Threshold cryptography is the process of encrypting the plain text into cipher text and decrypting the cipher text into original plain text using the fixed key and math function. Converted data code can be securely transmitted over a network. Here the actual content is converted into Hex-code for transmission.

VII. CONCLUSION

Terminode routing aims to support location-based routing on irregular topologies with mobile nodes. It achieves its goal by combining a location-based routing method with a link state-based mechanism. Further, it introduces the concept

of anchors, which are geographical points imagined by sources for routing to specific destinations, and proposes low overhead methods for computing anchors. Last, a special form of restricted search mode (Restricted Local Flooding, RLF), solves problems due to the inaccuracy of location information, in particular for control packets. The performance analysis shows that, in large mobile ad hoc networks, terminode routing performs better than MANET-like, or existing location-based routing protocols. It does so by maintaining its routing overhead low and by efficiently solving location inaccuracies.

Future Enhancement

A Mobile Gateway has been developed that uses a cellular network for the connection. It handles the challenges that had to be solved to realize this interconnection and describes a way how to connect two IPv6 networks over an IPv4 infrastructure. Different levels of mobility are described. Mobility within the ad hoc domain and between different Mobile Gateways of this ad hoc domain is handled using an enhanced AODV routing protocol. Mobility of the whole ad hoc network is handled by the mobility mechanisms of the cellular network and finally the seamless mobility of single ad hoc nodes is realized using two interfaces and a modified MobileIPv6 implementation.

REFERENCES

[1] Donggang Liu, Peng Ning and Wenliang Du, "Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks," 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), Columbus, OH, 2005, pp. 609-619.

[2] Z. Ren, W. Li, Shaoen Wu, Q. Yang and Lei Chen, "Location security in geographic ad hoc routing for VANETs", 2009 International Conference on Ultra Modern Telecommunications & Workshops, St. Petersburg, 2009, pp. 1-6.

[3] M. K. Prakruthi and M. Varalatchoumy., "Detecting malicious beacon nodes for secure localization in distributed wireless networks," 3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011), Bangalore, 2011, pp. 206-208.

[4] R. Jaiswal and S. Sharma, "Relative Cluster Entropy Based Wormhole Detection Using AOMDV in Adhoc Network," 2012 Fourth International Conference on Computational Intelligence and Communication Networks, Mathura, 2012, pp. 747-752.

[5] A. Atassi, N. Sayegh, I. Elhajj, A. Chehab and A. Kayssi, "Malicious Node Detection in Wireless Sensor Networks," 2013 27th International Conference on Advanced Information Networking and Applications Workshops, Barcelona, 2013, pp. 456-461.

[6] T. Stephen John and A. Aranganathan, "Performance analysis of proposed mobile autonomous agent for detection of malicious node and protecting against attacks in MANET," 2014 International Conference on Communication and Signal Processing, Melmaruvathur, 2014, pp. 1937-1941.

[7] A. A. A. Silva et al., "Predicting model for identifying the malicious activity of nodes in MANETs," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 700-707.

[8] S. B. Geetha and V. C. Patil, "Elimination of energy and communication tradeoff to resist wormhole attack in MANET," 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, 2015, pp. 143-148.

[9] M. Arai, "Reliability Improvement of Multi-path Routing for Wireless Sensor Networks and Its Application to Wormhole Attack Avoidance," 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), Beijing, 2015, pp. 533-536.

[10] D. Sharma and R. Kumar, "Reviewing the impact of wormhole attack in MANET," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 336-341.

[11] N. Tsitsiroudi, P. Sarigiannidis, E. Karapistoli and A. A. Economides, "EyeSim: A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs," 2016 9th IFIP Wireless and Mobile Networking Conference (WMNC), Colmar, 2016, pp. 103-109.

[12] M. Khanafer, Y. Gahi, M. Guennoun and H. T. Mouftah, "A Review of Intrusion Detection in 802.15.4-Based Wireless Sensor Networks," 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), Beijing, 2016, pp. 95-101.

[13] M. Bendjima and M. Feham, "Wormhole attack detection in wireless sensor networks," 2016 SAI Computing Conference (SAI), London, 2016, pp. 1319-1326.

[14] N. Devi and R. Sunitha, "Detection of malicious node using improved CONFIDANT technique in Ad-hoc Networks," 2016 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, 2016, pp. 604-610.

[15] C. Gupta and P. Pathak, "Movement based or neighbor based tehnique for preventing wormhole attack in MANET," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-5.

[16] A. Akila, D. Mahalakshmi and C. Saranya, "Recovering system recital by noticing wormhole attack," 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), Pudukkottai, 2016, pp. 1-5.

[17] A. E. Fawzy, A. Amer, M. Shokair and W. Saad, "Four-layer routing protocol with Location based Topology Control of active nodes in WSN," 2016 11th International Conference on Computer Engineering & Systems (ICCES), Cairo, 2016, pp. 66-72.

[18] L. Yang, C. Ding and M. Wu, "Location Similarity Based Replica Node Detection for Sensor Networks," 2016 9th International Symposium on Computational Intelligence and Design (ISCID), Hangzhou, 2016, pp. 56-59.

[19] Y. Guo, H. Ge, J. Huang and S. Li, "A General Strategy for Solving the Stochastic Point Location Problem by Utilizing the Correlation of Three Adjacent Nodes," 2016 IEEE First International Conference on Data Science in Cyberspace (DSC), Changsha, China, 2016, pp. 215-221.

[20] W. Liu, K. Nakauchi and Y. Shoji, "A location-aided flooding mechanism in community-based IoT networks," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2017, pp. 1-6.