Enhanced Multipath Routing using Energy Efficient Reliable Routing with Intrusion Tolerance in Mobile Wireless Sensor Networks

Singam Reddy Pallavi[1], N. Maneiah[2]
[1]*M.Tech (CSE), Dept. of CSE, Modugula Kalavathamma Institute of Technology for Women, Rajampet, Kadapa*
[2]*Assistant Professor, M.Tech. Modugula Kalavathamma Institute of Technology for Women, Rajampet, Kadapa*

***Abstract*- Enhanced Multipath Routing using Energy Efficient Reliable Routing with Intrusion Tolerance in Mobile Wireless Sensor Networks provides a huge rely on cooperation providing all participating nodes. Due to open medium and wide area networks usually there will be various vulnerable attacks which make various damages to the network topology and other activities of the network. The main contribution of the paper is to control various attacks and redesign the protocols in order to detect malicious and selfish nodes and provide cooperation through co-operative algorithm which provides centralized monitoring and management point. Providing security is a very critical problem as wide and open in nature, though many algorithms are designed in exhibiting the misbehaviors of nodes and controlling the curcial role of selfishness and trustiness. Due to open structure and very limited battery energy with some nodes may not cooperate correctly. This paper proposes a new Intrusion Detection System provides malicious node controlling, selfish node activities and trustiness and providing energy consumption activities. The paper reduces energy consumption and controlling energy hacking by moving the computation.**

I. INTRODUCTION

Enhanced Multipath Routing using Energy Efficient Reliable Routing with Intrusion Tolerance in Mobile Wireless Sensor Networks is a wireless network and autonomous system providing communication with mobile hosts and devices connected by wireless links. As wireless transmission range of each node gets executed by multi-hop packet forwarding. As the network is well established for various missions and critical applications such as communication, military operations providing enhanced communication and data sharing. As open wide and large networks there is lack of authorization facilities and volatile network topology we have every hard to detect malicious nodes [4,5] in WSNs doing various vulnerable to attacks. All the mobile hosts and devices are battery powered and limited resources which are heavy weight security solutions undesirable [7]. In wireless networks we have different types of malicious attacks that are to be identified and controlled in the same way they also check the battery resources with selfish nodes and trusted nodes for providing enhanced security. This paper provides and deals with Denial of Service Attacks by a Trusted Node and Selfish node with common form of attack which decreases the network performance.

As wireless networks provides policies with various nodes forward needed with better policies controlling and providing Energy Activities with Trust and Selfish Node Activities Depending on their user and node motivation we can categories the nodes in three categories i.e., Firstly discussing about Malevolent Nodes which won't compromise the security of the WSN or other nodes. These node actions are directly or indirectly show the effect on their own maximization benefit. Secondly we discuss about selfish nodes which forward's other packets with maximizing their benefit with all expense by providing advantage to the same node and finally discussing about trusted node which provides information of next consequent node status which are intentionally misbehaved or malevolent information about the nodes.

The energy consumption and energy attacks will intend to directly damage other nodes and the route

and also reduces the battery life, CPU cycles with available network bandwidth to forward packets in a secured and safe way, as the selfish node want to preserve their own resources we extend the selfish node with trusted node while using various services of others and consuming their resources and other energy of the nodes. In this paper we provide detecting routes and forwarding data packets with concept of energy consumption using trusted node and also consumes local CPU time, memory, network-bandwidth, and last but not least energy. Therefore there is a very strong motivation for each node to deny packet forwarding to other nodes based on the trust activity of the corresponding node and at the same time we also control the energy activities for all the nodes. According to the proposed attacking algorithm or technique the selfish and trusted node can be defined in three different ways

In the first way we take all the nodes participation in route discovery and route maintenance providing acceptance and refuses of forwarding data packets to its corresponding nodes. In the second way we provide various route discovery activities in data forwarding with the acceptance of the node in pre finding the trust activity of its corresponding node and provide effective resource controlling and transmission of data packets in secure way. Finally the node can behave properly with safe energy levels providing various threshold between various nodes and controlling energy level falls with behave like node or required type.

One of the immediate effects of node misbehavior activity and failures in wireless Senosr networks is the node isolation and communication problem due to the fact perfect communication between nodes are completely dependent between with nodes in throughout on routing and forwarding packets. In providing the presence of selfish and trusted node is a direct cause for node isolation concept and network partitioning technique, which further affects network survivability and usage among the interconnected nodes. This paper traditionally discuss about node isolation refers to the a novel phenomenon in which nodes have no (active) neighbors; whowever, we will show that due to the presence of selfish node, a node can be isolated even if active neighbors are available [2].

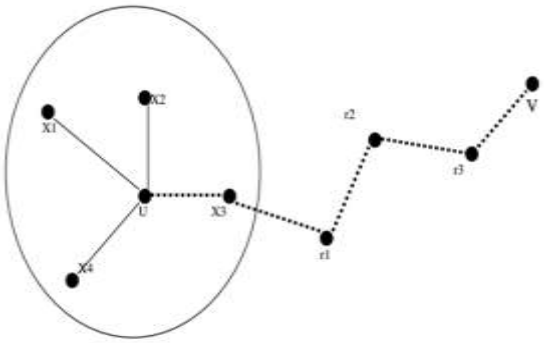

Fig 1: A hybrid WSN with routes to/from the gateway: very few nodes (grey) actually have to forward other nodes' data.

In Fig.1, we show Node x3 is suppose to be a selfish node where node u shows and initiates a route discovery to the corresponding node v were the selfish neighbors x3 may be reluctant to broadcast the information to the route request from the node u. In the proposed case x3 is a failed node and it is possible for x3 node to control packets, but the proposed situation is very worse since u node may select x3 node as the next corresponding hop to send data to it. Consequently the x3 node may discard all the data packets via it and the communication between u and v cannot be proceed. Here we discuss when all the corresponding neighbors of u are selfish the u is unable to establish a secure communication with other nodes at proposed distance having more than one hop away. In the proposed case, we say that the entire node is to be isolated by its selfish neighbors.

Now we discuss and describe various possible attacks on WSNs. Various WSNs and its protocols have intentionally and general attacks which are to be discussed before providing the project security activities. Coming to Passive Attacks which are eavesdropping and simplest attack on wireless network is eavesdropping attack, here a very minimal preparation is required but cannot be detected and this category is subdivided into content communication attack and infra-structure meta data attack, which includes a attack on protocol and its options to reduce energy resources of node. Various amount and distribution of communication with identifying location and content eavesdropping can still detected with traffic patterns among the nodes. In the proposed theory we could not avoid sending of messages between nodes but in the proposed mobile

environment we have infeasible due to energy constraint.

When discussing about policy activities of WSN which disclosure the information and location node's information might be considered a successful security breach and coming the non participation of WSN a node cloud not simply refuse to forward other node's connection when it is treated as un trusted node and we have two alternatives one the node not responding to route request is selfish behavior but having not having impair in the net as suboptimal activities are found in the route. When the node does not respond to route request we have silent discard of data which is it be supposed and forwarded to other node elimination the trust activity.

When discussing about active attacks where denial of service and enough resources on attacker is processed to destroy the energy activity of the node so that node cannot communicative with other nodes. Especially for mobile devices or clients we have vulnerable to denial of service attacks because their energy reserves are fastly drained off. Here we also have another possible approach to send large data to particular node and making the node energy drain and make the node to sleep. Direct attacks drains the energy and manipulates data activities.

When we discuss about Black hole attack where a node route is diverted to longest route and changes the shortest path to longest path disturbing existing routes so that more energy and time is used in transmission of data, traffic is increased and energy is consumed. This also leads to dropping of packets which is also called grey hole attack or various attacks on traffic and its contents.

An another attacks is Sybil attack in which one malicious node is simulated with number of Independent nodes where the basis of log of maniupations are done on routing decisions distributing the route activities..

II. LITERATURE SURVEY

Several methods proposed to defend these attacks and we have studied various related work for reference of designing a novel and advanced selfish and trusted technique. The studied information is described below.

Farooq Anjum et al. [1] in his paper he proposed a new approach in detecting intrusions in mobile and Senosr networks. Anand Patwardhan et al. [2] in his paper he proposed a new secure routing protocol for AODV over Internet Protocol Version 6 (IPv6) and further enhanced by a routing protocol with independent activity of intrusion detection and automatic response system for mobile Senosr networks. Chin-Yang Henry Tseng [3] author has proposed full distributed intrusion detection with four new activities for WSN which has self reasoning activities. Tarag Fahad and Robert Askwith [4] provided detection activities and conservation moning algorithm for detecting selfish nodes in WSNs.

Panagiotis Papadimitratos and Zygmunt J. Haas [5] proposed cryptography secure message transmission protocol with single path transmission and automatic configure to avoid transmission failures. Ernesto Jiménez Caballero [6] study provides various attacks against routing systemand various against the routing system. Yanchao Zhang et al. [7] paper provides the study of credit-based SIP called Secure Incentive Protocol which stimulate cooperation in packet forwarding for infrastructure less WSNs.

Li Zhao and José G. Delgado-Frias [9] authors proposed MARS technique for detecting misbehavior and controlling mitigate adverse effects in Mobile Senosr networks. Patwardhan et al. [10] in this paper he has discussed threshold based intrusion detection system with secure routing protocol Madhavi and Tai Hoon Kim [11] have proposed Mobile Intrusion Detection System with multi-hop Enhanced Multipath Routing using Energy Efficient Reliable Routing with Intrusion Tolerance in Mobile Wireless Sensor Networks wireless networks for secure routing and data transmission which detects nodes misbehavior and inconsistency in packet forwarding between intermediate nodes. Syed Rehan Afzal et al. [12] have projected and modified the existing protocols with secure on demand routing protocol. Bhalaji et al. [13] have explored with a relationship concept which calculates the trust units using DSR protocol. Azal et al. [12] have projected various security problems and attacks in existing routing protocols with a new secure on demand routing protocol called RSRP which is providing confiscates and solves the problems mentioned in the existing protocols. Moreover, unlike the proposed protocol by Ariadne is efficient in broadcast authentication

mechanism which is having no requirement with synchronization and facilities instant authentication.
Muhammad Mahmudul Islam et al. [15] have explored a possible new technique of a link level security protocol to be deployed SAHN called Suburban Enhanced Multipath Routing using Energy Efficient Reliable Routing with Intrusion Tolerance in Mobile Wireless Sensor Networks Network. Here the various security aspects and timing works with LLSP is suitable for link level security in mobile Senosr wireless networks. Shiqun Li et al. [16] have projected that the security issues of wireless sensor networks and minimized computations and communication overheads of light weight using less energy And in particular propose an efficient link layer security scheme. They have also devised a novel padding technique, enabling the scheme to achieve zero redundancy on sending encrypted/authenticated packets. As a result, security operations incur no extra byte in their scheme. Stefan Schmidt et al. [17] have proposed security architecture for self-organizing mobile wireless sensor networks that prevented many attacks these networks are exposed to. In addition, it has limited the security impact of some attacks that cannot be prevented. They analyzed their security architecture and they have showed that it has provided the desired security aspects while still being a lightweight solution and thus being applicable for self-organizing mobile wireless sensor networks

III. MOTIVATION

The main motivation for our work is to reduce the limitations of current IDS systems and address a new novel technique in providing advantage of the mobile device paradigm. Here we address and show solutions to various limitations which are earlier proposed and having some defects we show selfish routing with trust node management and energy controlling to reduce the false positive rate and provide a good reputation based scheme for increasing the network performance and scalability. The proposed technique shows good scalability for centralized approach in reducing Intrusion attacks on routing, between nodes and energy activities. By using Mobile Agent the scalability may increase that enhance the network performance.As the WSN is open medium and wide area which requires centralized controlling but due to various other components in local exchanging it is not able to secure centralized authorization of previous IDS the IDS cannot perform efficiently.

IV. PROPOSED WORK

The main objective of the projected project is the find the malicious nodes and improves the performance of nodes, network by selfish and trusted routing network. The assumptions regarding the proposed work are listed below

1. We construct and interact with 1 to many hop neighbors directly with intermediate nodes using multi hop packet forwarding.
2. Here all the nodes will have unique id in the network which is automatically assigned to the existing nodes.
3. We generate and transmit message from source node and sends to router.
4. The router moves the information towards shortest path controlling selfish activities with trusted routing and controlling energy activities and discovers a malicious node, instead of moving forward, it sends a report to the source node. In Fig 2 we show the data transmission between node 1 and node 10 where node 1 is source node and node ten is destination node and considering neighbor list 3,4,5,8 and 9. all its neighbor nodes shown in Table 1.

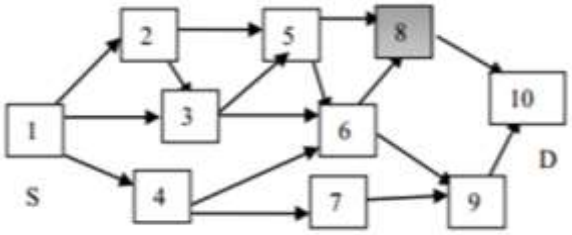

Figure 1: A WSN of 10 nodes

Table 1: Neighbor Nodes Information

Node ID	Neighbors
6	3,4,5,8,9

The above figure shows various neighbor nodes to send and receive the message from source to destination to see if it is the intended recipient. If yes it sends a message to the next consequent node and the current sequence of route node 3, 4, 5, 8, 9 maintain the sequence number in the SnT and

sequence numbers are generated randomly in simulation shown in Table 2.

Table 2: DST Sequence Information

Node ID	DST_Seq
3	10
4	7
5	8
8	6
9	5

When an intermediate node receives a message it checks if the difference between the Dst node and Seq node to present in the route for transmitting a message and the sequence no present in its table is greater than some predefined threshold value? if so then the intermediate node stops forwarding the message and mark the node as „M" or malicious in the status table(ST) and send a notification message(NM) to source node along with the malicious node"s id and neighbor list of the malicious node. Node 6 keeps track of the status of each neighbor node in the ST whether it is a safe node or a malicious one. Suppose we consider node 8 as malicious. The ST is shown in Table 3.

Table 3: Status Table Information

Node ID	DST_Seq
3	S
4	S
5	S
8	M
9	S

The neighbor nodes of node 8 are 5, 6, 10.Then these nodes after receiving the Further Detection message, broadcast a requested message by setting destination address to source node"s address. If it receives a requested message from the malicious node, it sends a Test packet (TP) to the source node via malicious node, and at the same time it sends a Acknowledgment Packet (AP) to source node(SN) though some other route. Then the source node waits for „wt" time until it receives the entire test and acknowledgement packet. If, SN receives a TP, it updates the Flag Table (FT) by adding the source node id to the table and set the flag of the node as „Y" and if an AP is received set the flag as „N" and update the count field. Table 4 shows the Flag Table maintained by node 1 is as follows:

Table 4: Flag Table

Node ID	DST_Seq
5	N
6	N
10	N

If all the entries for the malicious node are „N" then source node updates the status table (ST) by adding the MN"s id to the ST and making the status as „B" i.e. Black hole. After confirmation of the Black hole node the ST of source node 1 is given in Table 5.

Node ID	DST_Seq
7	B

V. ALGORITHM

Begin
Step1 the source node N0 sends packet to the destination node N6.
Step2 Start Timer T.
Step3 Wait for the acknowledgement from destination node.
Step 4 increase T by unit time.
Step 5 if T>Tout then
Goto step 6
Else
Goto step 3
Step 6 The node S generates Mobile Agent(MA) and provides it's own ID and
send it to the next hop node
Step7 The mobile agent observe for ith node the number of packet receive from
neighbor node j and compute CPR(i, j
Step 8 MA compute CPF(i,j)for the ith node
Step 9 MA compute Pdr(I,j) for the ith node at tth instance
Step 10 If the ratio is less than threshold for ith node
Then
The agent moves to the next hop node
decrase hop count by 1
Else
Agent reports the malicious activity to the source node
End

VI. PERFORMANCE ANALYSIS

The projected is system provides better performance of network routing, energy saving, selfish controlling and trusted routing by comparing the performance of old system we can say the simulation metrics shows better result and observation with enhanced performance of the network in presence and

controlling the malicious nodes. The presence of mobile network performance we can improve the network by preventing malicious nodes. Initially the Average Throughput of Receiving Packet is same implies that he network is free from network at that time instant. As the packet size increases the throughput decreases means due to packet overhead the throughput decreases.

VII. CONCLUSION AND FUTURE SCOPE

We can conclude that mobile Enhanced Multipath Routing using Energy Efficient Reliable Routing with Intrusion Tolerance in Mobile Wireless Sensor Networks network are suffering from various types of intrusions, denial of service attacks by selfish node is one them. In wireless networks especially in mobile Senosr networks a mobile agent will be traveling through the network gathering various vital information, as open medium and large networks we have many thresholds and attacks on energy, route and other activities of the network. The project proposes a novel technique with computation complexity and minimizes overhead by controlling various attacks and reducing the refusing of packet delivery among the neighbor nodes. The nodes are also free from performing the computation. This feature of our proposed scheme increases the efficiency of each node thereby increasing the overall performance of the network.

REFERENCES

[1] Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar "Signature based Intrusion Detection for Wireless Enhanced Multipath Routing using Energy Efficient Reliable Routing with Intrusion Tolerance in Mobile Wireless Sensor Networks Networks: A Comparative study of various routing protocols" in proceedings of IEEE 58th Conference on Vehicular Technology, 2003.

[2] Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis "Secure Routing and Intrusion Detection in Senosr Networks" Third IEEE International Conference on Pervasive Computing and Communications, March 2005.

[3] Chin-Yang Henry Tseng, "Distributed Intrusion Detection Models for Mobile Senosr Networks" University of California at Davis Davis, CA, USA, 2006.

[4] Tarag Fahad and Robert Askwith "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks", in proceedings of the 7th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, June 2006.

[5] Panagiotis Papadimitratos, and Zygmunt J. Haas, "Secure Data Communication in Mobile Senosr Networks", IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006.

[6] Ernesto Jiménez Caballero, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem", 2006.

[7] Yanchao Zhang, Wenjing Lou, Wei Liu, and Yuguang Fang, "A secure incentive protocol for mobile Senosr networks", Wireless Networks (WINET), vol 13, No. 5, October 2007.

[8] Liu, Kejun Deng, Jing Varshney, Pramod K. Balakrishnan and Kashyap "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in WSNs", IEEE Transactions on Mobile Computing, May 2007.

[9] Li Zhao and José G. Delgado-Frias "MARS: Misbehavior Detection in Senosr Networks", in proceedings of IEEE Conference on Global Telecommunications Conference,November 2007.

[10] A.Patwardhan, J.Parker, M.Iorga, A. Joshi, T.Karygiannis and Y.Yesha "Threshold-based Intrusion Detection in Adhoc Networks and Secure AODV" Elsevier Science Publishers B. V., Senosr Networks Journal (ADHOCNET), June 2008.

[11] S.Madhavi and Dr. Tai Hoon Kim "AN INTRUSION DETECTION SYSTEM IN MOBILE ADHOC networks" International Journal of Security and Its Applications Vol. 2, No.3, July, 2008.

[12] Afzal, Biswas, Jong-bin Koh,Raza, Gunhee Lee and Dong-kyoo Kim, "RSRP: A Robust Secure Routing Protocol for Mobile Senosr Networks", in proceedings of IEEE Conference on Wireless Communications and Networking, pp.2313-2318,April 2008.

[13] Bhalaji, Sivaramkrishnan, Sinchan Banerjee, Sundar, and Shanmugam, "Trust Enhanced Dynamic Source Routing Protocol for Adhoc Networks", in proceedings of World Academy Of Science, Engineering And Technology, Vol. 36, pp.1373-1378, December 2008

[14] Meka, Virendra, and Upadhyaya, "Trust based routing decisions in mobile ad-hoc networks" In Proceedings of the Workshop on Secure Knowledge Management, 2006.

[15] Muhammad Mahmudul Islam, Ronald Pose and Carlo Kopp, "A Link Layer Security Protocol for Suburban Ad-Hoc Networks", in proceedings of Australian Telecommunication Networks and Applications Conference, December 2004.

[16] Shiqun Li, Tieyan Li, Xinkai Wang, Jianying Zhou and Kefei Chen, "Efficient Link Layer Security Scheme for Wireless Sensor Networks", Journal of Information And Computational Science, Vol.4, No.2,pp. 553-567, June 2007.

[17] S. Schmidt, H. Krahn, S. Fischer, and D. Wätjen, "A Security Architecture for Mobile Wireless Sensor Networks", In proceedings of First European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), August 2004.

[18] M. O. Pervaiz, M. Cardei, and J. Wu, " Routing Security in Ad-hoc Wireless Networks" Network Security , S. Haung, D. Maccallum, Springer, 2008.

[19] B. Awerbuch, D. Holmer, C. Nita-Rotaru, " An On-Demand Secure routing protocol Resilient to Byzantine failures", Proceedings of ACM workshop on wireless security 2003, Sep. 2003.

[20] K. Sanzgir, and B. Dahill, " A secure routing Protocol for ad-hoc networks", Proceeding of the 10th IEEE International Conference on Network Protocols, 2002, pp.1-10.