ROUTING SECURITY AGAINST CRIPPLE ATTACKS IN MOBILE AD HOC NETWORK

C.DANIEL NESA KUMAR[#1], Dr. V. SARAVANAN[#2]

[#1]*Ph.D-Research Scholar, Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India.*

[#2]*Professor and Head, Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India.*

Abstract - In the recent trend Mobile Ad hoc Networks place a vital role. But those Mobile Ad hoc Networks suffers from lots of security threads. The proposal considers a new class of resource consumption attacks which is defined and named as Energy drain attacks which is not clearly defined earlier in routing protocols. The existing system used rate limiting and revocation methods to prevent energy draining issues. But those solutions failed to find the exact solution for the Energy drain attacks. The proposed network routing protocol provably prevents data from Energy drain attacks by verifying packets consistently and makes progress toward their destinations with the verification and forwarding scheme. The existing system is not offered a fully satisfactory solution for Energy drain attacks during the topology discovery phase, so the system implemented a new scheme named as **"Energy Booster against Energy Consumption Attacks"** with some perception about energy limitations due to damage. This protocol enables the energy boost-up process when there is low energy. The proposed technique tries to prevent the data from attacks and retransmits on the best optimal path. The proposed technique overcomes the data from damage and this uses optimal routing techniques and dynamic topology changes. The consequences had proved that the proposed scheme affords an unsurpassed resolution for both energy suckers and cripple attacks in mobile ad hoc networks.

Keywords - *MANET, Secure Routing, Cripple attacks.*

I. INTRODUCTION

Existing work on secure routing endeavors to guarantee that opponent cannot origin the pathway for sighting to revisit a worthless network path, but energy suckers do not interrupt or amend the discovered paths; surrogating the existing network paths along with protocol complaint messages. Protocols may increase the power competence since they reside on their supportive node deeds and retreating wicked actions has been impossible. Existing wireless network have exaggerated by other such threats namely Carousel attack, in which the opponents will compile the packets in such a way intentionally to initiate routing loops and so the attackers may send packets in circles continuously to drain the energy of particular node. Finally the targets source routing protocols will make use of the limited verification of message headers and will allow a single packet in order to revert the same set of nodes.

Another attack is **Stretch attack; in this attack** an adversary constructs artificially long routes, potentially traversing every node in the network. This increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. The third type of attack is **Cripple Attack; here a**n adversary constructs or creates a fake node and routes artificially, and makes the node to pretend the path is shortest. This increases packet transmission energy, causing packets to be processed by more number of transmission and process time. This type of process may make the node become idle. The major issues of the impact of this attack are, Power Outages, Due to environmental disasters, loss in information. Lost in productivity and it creates various other types of attacks such as DOS attacks and Security level is very low.

II. PROBLEM DEFINITION

Consumption of resources assails the energy which makes the routing protocols to immobilize mobile ad hoc networks eternally. This can be achieved by exhausting the usage of battery power. It was resulted that these attacks are independent on any of the protocols but also result in scrawny in a number of popular protocol classes. Depending on the position of adversary, energy of the network disbursement will increase rapidly. The proposed work has been initiated in cause of making the routing protocol which limits the smashes resulted from Energy drain attacks which is done by confirming the reliability and evolutes the path from source to destination and there by reduces the damage. Origination of damage limits and resistance for discovering topology and handling of mobile networks will take part.

III. RELATED WORKS:

Owing to their ad hoc nature, wireless ad hoc networks will expose to denial of service (DoS) attacks [1], which explore to augment reliability.

This paper [2] addressed the security issues, as especially damaging form of DoS attack, called PDoS (Path-based Denial of Service). In a PDoS attack, the opponent will conquer the sensor nodes away by overcoming a multi hop end-to-end communication path with iterated packets or fake ones. In order to avert this end-to-end communication a one-way hash chain mechanism can be used. The pro of the paper is lightweight, endures heavy packet losses, and can easy implementation techniques in current Mobile ad hoc networks. The PDOS suffers from difficult burden on the sender, who must know a priori each node in the path in order to send the relevant verification information.

In the paper [3] discusses various protocols proposed for security of wireless networks by different researchers. SNEP structures with the basic features of another protocol named as SPINS, for which the ultimate make over is for secure key distribution in mobile ad hoc networks. SNEP is utilized for the traditional methodologies for authenticating sensor node, data confidentiality and data integrity. Drawback of this protocol is lower data freshness. SNEP protocol works in such a way by employing the shared counter for semantic reliability and not for initial vectors. For encryption of data the plain text can be ciphered with CTR encryption algorithm. In case of sending or receiving the cipher blocks, it is mandatory and responsible for both the sender and receiver to update the shared counter. Therefore, sending counter is alone not responsible for transmitting the cipher blocks. Each message should contain own Message Authentication Code (MAC); which can be computed from cipher data with the help of CBC-MAC algorithm. On the other hand, when the receiver node receives the data, the comparison between the recomputed MAC and received MAC will take place.

Paper [4] proposed a new algorithm know as REWARD for security against black hole attack as well as malicious nodes. It works on geographic routing. There are two different kinds of broadcast messages used by REWARD.

1. MISS message helps in the identification of malicious sensor nodes.
2. While the second message SAMBA is used to recognize the physical location of detected black hole attacks and broadcast that location.

Reward can access the broadcast inter radio conduct to scrutinize the neighbor node's communication and detect black hole attack. If any sensor misbehaves, that data will be maintained in a distributed database which will also save its information for future use. Finally the major drawback of this protocol is utilization of huge energy.

In paper [6] occurrence of a statistical en-route filtering technique will control attacks on conciliation sensor nodes, in which the conciliated node may cause the erroneous report in the network that may result in weakening of resources at sensor nodes and also may cause false alarms. In order to find out such flawed reports in the network, statistical En-route filtering can be incorporated. For this purpose message authentication code (MAC) is used to check the validity of each message.

Energy drain attacks [5] are not a protocol-exact, which do not concern on design methodologies, implementing faults of particular routing protocols, but takes account onto general properties of protocol classes, i.e., link-state, distance-vector, source routing and geographic, beacon routing. This won't rely on submerging with large amounts of data; while tries to convey as little data as possible to accomplish the largest energy drain which will thwart a rate limiting solution. Utilization of protocol-complaint messages by energy suckers, those attacks are very difficult to detect and prevent.

The paper [5] do not imply that power draining itself is story, but rather that these attacks have not been thoroughly defined, assessed, or mitigated at the routing layer. A very early mention of power exhaustion can be found in [7], as "sleep deprivation torture." As per the name, the proposed attack prevents nodes from entering a low-power sleep cycle, and thus drains their batteries faster.

Latest research on "denial-of-sleep" only considers attacks at the MAC layer [8]. Additional work mentions resource fatigue at the MAC and transport layers [9] but only offers rate limiting and elimination of insider adversaries as potential solutions.

Malevolent cycles i.e. routing iterations, specified in [10], no suspicious activities are taken into account excluding the method of increasing the efficiencies of underlying MAC and routing protocols else switching process. When considered with non-power constrained systems, diminution of resources namely memory, CPU time, and bandwidth may lead to problems.

A popular example is the SYN flood attack, wherein adversaries make multiple connection requests to a server, which will allocate resources for each connection request, eventually running out of resources, while the adversary, who allocates minimal resources, remains operational (since he does not intend to ever complete the connection handshake). Such attacks can be defeated or attenuated by putting greater burden on the connecting entity.

These solutions place minimal load on legitimate clients who only initiate a small number of connections, but deter malicious entities who will attempt a large number. Note that this is actually a form of rate limiting and not always desirable as it punishes nodes that produce heavy traffic but may not send much total data over the lifetime of the network.

Summary:

This examines that security measures to prevent Energy drain attacks are involved in the right way to those used to protect routing infrastructure, and so existing secure routing protocols do not protect against Energy drain attacks. Existing work on secure routing attempts to ensure that adversaries

cannot cause path discovery to return an invalid network path, but Energy suckers do not disrupt or alter discovered paths. Protocols maximize the efficiency which determines the cooperative node and malicious actions.

To prevent data from attackers in MANET, the system implemented a new scheme named as **"eSI_eMAX (energy Sucker Identifier_ energy Maximization)"** with some perception about energy limitations due to damage. This scheme enables the energy boost-up process when there is low energy. The proposed technique tries to prevent the data from attacks and retransmits on the best optimal path. The proposed technique overcomes the data from damage and this uses optimal routing techniques and dynamic topology changes. The scheme can protect data from the Energy drain attackers and increases the security level and Boost up the battery power.

IV. PROPOSED METHODOLOGIES

In the proposed system each node maintains routing information for all known destinations. In the proposed system the routing information must be updated periodically. The main contribution of the proposed work is as follows.

4.1 Contributions:

1. Energy and Path aware Routing protocol (EPR)
2. Energy Sucker Identification algorithm
3. Energy Maximization algorithm
4. Anti Back Tracking method (ABT)

The EPR routing protocol has been proposed. This provides real-time end-to-end guarantees in WSN. The protocol requires each node to maintain routing information about its neighbors and uses geographic and attack aware forwarding to find the best paths. In addition, EPR strive to ensure certain energy, time for each packet in the network so that each application can estimate the end-to-end delay and energy for the packets. Moreover, EPR can provide energy when the network is compromised.

The routing module in EPR is called energy and node aware routing to avoid energy based attacks. The proposed system performs the hop by hop verification to prevent energy drain attacks.EPR includes hop attestations, increasing the size of every packet, and thus radio power. The information exchange mechanism collects information about the nodes and their energy and distances. Delay estimation at each node is basically made by calculating the elapsed time when an ACK is received from a neighbor as a response to a transmitted data packet. By looking at the delay values, the proposed routing protocol selects the node, which meets the distance and energy requirement. If such a node cannot be found in the network, the relay ratio of the node is checked. The proposed system provides an anti backtracking routing method. The anti backtracking property, satisfied for a given packet if and only routes. This already means the adversary cannot perform carousel or stretch attacks, no node may unilaterally specify a suboptimal path through the network. This section describes the anti backtracking based routing protocol for fast and secure transmission to obtain security against stretch, Carousel and cripple attacks.

Steps:

1. initialize every node
2. Register and active a node n1, n2…Nn.
3. initial energy analysis
4. Source generates data=send(source, destination, path , attestation, ABT id) where ABT is anti back tracking id which is a temporary id
5. For each node , (EPR- message)
   Send EPR(sender, receiver, seqno, abt id)
   Analyze the node by their energy and distance
6. if (Node seq no == largest seq no)
   Verify routing table.
7. Sender transmits to the verified forwarder node
8. apply anti backtracking method
9. evaluate energy
10. if energy is sufficient then forward else perform energy maximization algorithm
11. monitor the node behavior and elect best forwarder
12. report and update the routing table

This approach incorporates the solution against energy based attacks and data security with EPR routing Protocol and ABT. This protocol provides a secure and guaranteed transmission of data. To accomplish secured communication anonymous key is generated. To obtain reliable transmission routing scheme is used. In this approach the id for data packets and are randomly generated and the adversary cannot be able to differentiate the path details with the data packets. To achieve the fast and secure transmission two phases are used in this method: ABT key construction and Table driven routing.

V. EXPERIMENTS AND RESULTS

Implementation Process:

- Node creation
- Protocol Implementation
- Results

Node creation:

A node is an "entry" point to a series of classifiers. The address classifier contains a slot table for forwarding packets to foreign nodes, but since the proposed routing is not used, all packets not destined for this node (and hence forwarded to the port classifier), which will be forwarded to the default target which in turn summits to a routing agent. When the packets are

intended for port 255 are termed as routing packets which is frontward to the routing agent.

Protocol Implementation:

Routing protocol provides more reliable, less bandwidth-intensive, but also more complex and compute- and memory-intensive.

Route discovery process starts when a source node does not have routing information for a node to be communicated with. Route discovery is initiated by broadcasting message.

Simulation results:

Through the event driven simulator this sees final output through the Network animator window. The first step to use name is to produce the trace file.

The trace file contains topology information, e.g., nodes, links, as well as packet traces. As a result, internally reads information from a file and keeps only a of animation event information in memory. Its animation event has a fairly simple and consistent structure so that it cans many different visualization situations.

VI. PERFORMANCE EVALUATION & RESULT ANALYSIS

This section deals with the performance comparison of the systems such as PLGP, OEBP, and OEBP for energy suckers attack, detection and prevention.

A. Packet Delivery Ratio:

Packet delivery ratio is a ratio linking the packets reached at destination to the sum of packets transmitted from source. Performance of transmission is symbolized by the packet delivery ratio. If the delivery ratio of the packets is high, then the performance will also be high.

B. Average End –to –End Delay:

End-to-end delay is nothing but the time taken for transmitting the packets from sender to receiver. Average delay is the ratio between the time difference and the total number of packets received at the destination. When the average end –to –end delay is low then the performance is high.

C. Time Complexity:

The time complexity of an algorithm is measured as the time taken to execute a method or function by an algorithm for the given input. The time complexity of an algorithm is generally articulated using "big O" notation. Here the time complexity of OEBP is O (N) where the complexity is O (N) + 4.

PLGP imposes exaggerated setup price over OEBP, but compares favorably to in terms of packet forwarding overhead. Whereas path stretch will increase by an element of one.5-2, message delivery success while not resorting to localized flooding is improved: PLGP never floods, whereas OEBP should flood 5-10 p.c of packets depending on network size and topology PLGP conjointly demonstrates additional just routing load distribution and path diversity than OEBP. Since the forwarding part ought to last significantly longer than setup, PLGP offers performance comparable OEBP in the average case. OEBP includes path attestations, increasing the scale of every packet, acquisition penalties in terms of information measure use, and therefore radio power.

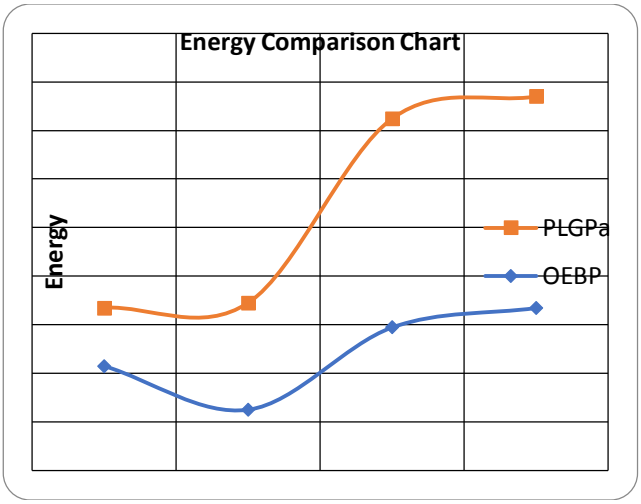

Figure: 1.0 comparison of damage with energy with secure forward routing.

While adding additional packet verification requires the necessities for intermediate nodes which results in amplifying the utilization of processors, total time taken and also extra power. The information measure overhead of our attestation theme is minimal, as chain signatures are compact (less than thirty bytes). Relatively, a minimum-size DSR route request packet with no route, payload, or further choices is twelve bytes; we have a tendency to used 512-byte knowledge packets in our simulations.

The above figure describes the performance comparison between the existing approaches and the proposed system. That result shows the effectiveness of the proposed system by using three parameters such as latency, throughput and security. The following chapter indicates the detailed results of the proposed system performance.

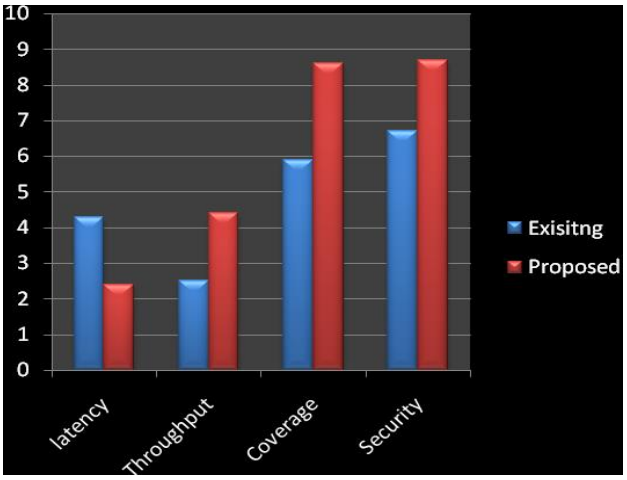

Figure 2.0 Performance Comparison

VII. CONCLUSION

In this paper, this has a propensity to delineate Energy drain attacks, a replacement category of resource utilizing attacks which access the routing protocols in order to disable contingent wireless device networks by reducing the battery power. This attack doesn't depend on the precise protocols or implementations, but depicts weak in a variety of standard protocol categories. This predisposes to view the variety of proof-of-concept attacks against the samples of existing routing protocols; meanwhile this employs weak adversaries and measures their attacks for accidently generated topology of thirty nodes. Replication results show that a scenario that the condition based on proposed protocol will reduce the energy based risk which will be against to the Energy drain attacks. Finally, the system has proposed to suspicion against a number of the forwarding-phase attacks and outline.

VIII. REFERENCES

[1]. A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[2]. Deng, Jing, Richard Han, and Shivakant Mishra. "Defending against path-based DoS attacks in wireless sensor networks." *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*. ACM, 2005.

[3]. Perrig, Adrian, et al. "SPINS: Security protocols for sensor networks." *Wireless networks* 8.5 (2002): 521-534.

[4]. [4] Z. Karakehayov, Using REWARD, to Detect Team Balckhole Attacks in Wireless sensor Networks Workshop on Real world Wireless Sensor Networks, (REAL WSN, 05) Stockholm, Swedan, June 2005.

[5]. [5] Vasserman, Eugene Y., and Nicholas Hopper. "Energy drain attacks: Draining Life from Wireless Ad Hoc Sensor Networks." *Mobile Computing, IEEE Transactions on* 12.2 (2013): 318-332.

[6]. [6] Fan. Ye, H. Luo, Songwu. Lu. L. Zhang. Statistical en-route Filtering of injected False Data in Sensor Networks IEEE Journal on Selected Areas in Communications, Vol-23, (4), pp. 839-850, April 2005.

[7] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks," Proc. Int'l Workshop Security Protocols, 1999.

[7]. [8] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.

[8]. [9] D.R. Raymond and S.F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, pp. 74-81, Jan.-Mar. 2008.

[9]. [10] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.