www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 12157-12162

Prevention And Elimination Of Vampire Attacks That Drains Life From WSN Using IDS

Archana Krishnan[1], Mr. Manoj. R[2]

[1]M-Tech Scholar, Department of Computer Science & Engineering,
College of Engineering Munnar, CUSAT
Munnar, Idukki, Kerala, India
akarchana34@gmail.com

[2]Asst. Professor, Department of Computer Science and Engineering,
College of Engineering Munnar, CUSAT
Munnar, Idukki, Kerala, India
manojmyd@gmail.com

Abstract: ***Mobile ad-hoc network is an infrastructure-less network in which the routing operation plays an important role. Due to the infrastructure-less nature of ad-hoc network, it has different issues like MAC layer, routing, security, network survivability etc. One of them is network survivability which needs more concern. It is the ability of a network keeping connected under attacks and failures in the design and performance of wireless ad hoc sensor networks. The large portion of research efforts concentrates on maximizing the network lifetime, where the lifetime of network is evaluated from the time of deployment to the point when one of the nodes has spent its limited power source and becomes in-operational – commonly referred to as first node failure. There is a class of resource consumption attacks called vampire attack which permanently disables the whole network by quickly draining nodes battery power. These types of attacks alter targeted packets by preparing long routes or misguiding the packets. Malicious nodes use false messaging, or alter routing information. This action affects the bandwidth and node battery power. This paper proposes a system that detects and eliminate the vampire attacks by using IDS and thus make the network live.***

Keywords: Denial of service, routing, security, ad-hoc networks, wireless networks, sensor networks, IDS

1. Introduction

Wireless ad hoc sensor network also called infrastructure-less network consists of a number of sensors spread across a topographical area. Wireless Sensor Networks (WSN) imparts different methods for sensing and disseminating information from various environments which provide the potential to serve many different applications. Each sensor node has a wireless communication capability and some level of intelligence for signal processing and networking of the data. It imparts a capable network infrastructure for many applications like military surveillance, medical care, environmental monitoring, etc. Due to their ad-hoc nature, wireless adhoc networks are concretely vulnerable to denial of service (DoS) [1] attacks and a great deal of research has been done to enhance indomitability. While these schemes can avert attacks on the network in short-term availability, they do not tackle attacks that have effect on long-term availability. The most common denial of service attack entirely depletes the nodes' batteries of the network. This is an occurrence of a resource depletion attack [2], with battery power as the resource of attention.

In this paper we consider how routing protocols, still those designed to be secure lack protection from these attacks, which we call as vampire attacks. These attacks are called vampire attacks because they drain the life from networks nodes. They are different from previously-studied reduction of quality (RoQ), Denial of service (DoS), and routing infrastructure attacks as they do not disturb direct availability, but somehow work over time to entirely disconnect a network. Previous work has been mostly restricted to other levels of the protocol stack, e.g. medium access control (MAC) or application layers, and to our discussion there is little discussion, and no complete survey or diminution, of routing-layer source enervation attacks. Vampire attacks are not specific to any protocol, in that they do not depend on design properties or implementation faults of specific routing protocols, but rather utilize common properties of protocol classes such as link-state, source routing, geographic, beacon and distance vector routing. Neither do these attacks depend on flooding the network with huge amounts of data, but try to transmit as little data as possible to attain the biggest energy drain, preventing a rate limiting solution. Because Vampires make use protocol-compliant messages, these attacks are very complicated to detect and prevent.

1.1 Overview

Here in this paper we evaluated the vulnerabilities of existing protocols to routing layer battery reduction attacks [14]. Existing work on secure routing attempts to confirm that an attacker cannot cause path discovery to return an invalid network path, but Vampires do not alter discovered paths instead of that it uses existing valid network paths and protocol compliant messages. Protocols that increase power efficiency

are also inappropriate because they depend on cooperative node behavior and cannot optimize out malevolent work. To bound the damage from Vampire attacks during forwarding of packets modify an existing sensor network routing protocol .The effect of Vampire attacks are considered on distance vector, link-state, source routing and beacon routing protocols also a logical ID-based sensor network routing protocol [13]. According to above stated protocols we view the covered protocols as an important subset of the routing solution that our attacks are likely to apply to other protocols.

All routing protocols employ at least one topology discovery period. Our attackers are malevolent insiders having the same resources and level of network access as honest nodes. Assailant location within the network is assumed to be fixed and random. This is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks. Smart assailant placement or dynamic node compromise would make attacks far more destructive. While for the remaining section of the project we will assume that a node is permanently disabled once its battery power is exhausted, considering nodes that recharges their batteries in the place, using either continual charging or switching between recharge and active cycles. In the case of continuous charging, power-draining attacks [14] would be effective only if the rival is able to consume power at-least as fast as nodes can recharge. Considering that packet processing drains at least as much energy from the victims as from the attacker, a continuously recharging rival can keep at least one node permanently disabled at the cost of its own functionality.

If vampire attack exists in the network, it will affect one node and drain its full energy and the particular node goes to dead state and then the vampire attack concentrates on next node and so on it affects all nodes in the network, as a result all nodes goes to dead state [15]. The vampire attack permanently disables or destroys the entire network.

Section II of this paper shows some of the related works that help in the modeling of this project. Section III explains the type of attacks that affect the stateless protocols (stateless- the nodes are unaware of the network topology) and the mitigation methods to detect and prevent such attacks. Section IV helps us to understand a clean state secure sensor network [8] and packet forwarding is studied in the presence and absence of a vampire. Section V explains about the proposed technique on securing the network from the malicious attack. Our implementation results in the efficient detection and elimination of vampire attack from the network. In order to detect and eliminating the vampire attack we are going implement certain Intrusion Detection System (IDS) based on the energy level constraints and the simulation results are also shown in section VII.

2. Related Works

Most of the research on this topic is revolved around security solutions using the layered approach. In layered approach the protocol stacks consists of the data link layer, physical layer, network layer, transport layer and application layer. These five layers and the three planes, i.e., the mobility management plane, power management plane, and task management plane jointly forms the wireless layered architecture. Researchers are being carried out to improve the energy efficiency of the wireless Sensor Networks. Some of the approaches are described. They are:

2.1 Denial of sleep attack

Michael Brownfield [3] discussed the energy resource vulnerabilities at MAC level. Denying of sleep effectively attacks each sensor node's critical energy resources and rapidly drains the network's lifetime so proposed a new GMAC protocol to control the sleep awake pattern of sensor nodes. G-MAC has several energy saving features which not only show promise in extending the network lifetime, but the centralized architecture makes the network more resistant to denial of sleep attacks. This scheme performs well in all traffic situations but deals only with MAC layer depletion attack. G-MAC divides a frame into a distribution period and a collection period.

2.2 Intrusion tolerant routing

The Jing Deng, Richard Han, Shivakanth mishra [4] proposed an Intrusion tolerant routing protocol for WSN. INSENS constructs a forwarding table at each node to facilitate communication between sensor nodes and base station. In INSENS each node shares a secret key only with the base station and not with any other nodes. This has advantage in case a node is compromised that an intruder will only have access to one secret key rather than the secret keys of neighbors and other nodes throughout the network. It also provides multi path routing and minimizes the communication, storage and computation requirements of sensor node at the expense of increased requirements at base station.

2.3 Cross-layer design approach

Fatma Bouabdullah, Nizar Bouabdullah, Raouf Bouabdullah [5] proposed a cross layer strategy that considers routing and MAC layers jointly. A network lifetime is defined as the time for the first node in wireless sensor network to fail. An effective routing protocol would drain energy uniformly and slowly among nodes leading to the death of all nodes nearly at same time. At routing level they proposed that sending data through multiple paths instead of using a single path so can balance energy consumption. At MAC level limits the retransmission over each wireless links according to its property and the required packet delivery probability, but this scheme does not considers any attack.

2.4 Opportunistic routing method

Xufei Mao,Shaojie Tang, Xiahua Xu & Huadong Ma[6] focused on opportunistic method to minimize energy consumption by all nodes but this method does not consider any attack at routing level. Opportunistic routing is based on the use of broadcast transmission to expand the potential forwarders that can assist in the retransmission of data packets. By this method nodes in the forwarder list are prioritized and the lower priority forwarder will discard the packet if the packet has been forwarded by a higher priority forwarder.

2.5 Optimal sleep-wake scheduling for Quickest

Intrusion Detection K.Premkumar and Anurag Kumar [12] proposed a protocol that uses markov decision process models to identify the malicious nodes quickly with the use of minimal set of sensor nodes in active state. By using a minimum number of sensor devices, it ensures that the energy outlay for sensing, computing and communication is minimized and so the lifetime of network is maximized.

2.6 Sleep deprivation attack

Tapaliana Bhattasali [7] proposed a frame work based on distributive collaborative mechanism for detecting sleep deprivation attack increased energy efficiency but does not considers routing layer. Sleep deprivation torture comes in the

form of sending useless control traffic and forces the node to forgo their sleep cycles so that they are completely exhausted and hence stop working. Here workload is distributed among components according to their capacity to avoid complete exhaustion of battery power. Packet transmission overhead may high in some cases and its main advantage is it enhances energy efficiency and network scalability.

2.7 Vampire attack

E.Y Vasserman & N. Hopper [8] proposed a new method for resource depletion attack at routing layer (Vampire attack), which permanently disable networks by quickly draining nodes battery power. Vampire attack is defined as the composition and transmission of a message that causes more energy to be consumed by the network than if a honest node transmitted a message of identical size to the same destination although using different packet headers. Here deals with 2 kinds of vampire attacks. They are stretch attack and carousel attack, then employs vampire attacks on an existing routing protocol PLGP during packet transmission phase [8]. PLGPa is the new protocol to avoid this attack. Here a check is made before forwarding any packet to next hop. The node checks whether the hop distances is increasing or not, thus each node validates the path and can avoid the chance of attack.

Table 1: Classification of different types of attacks

Sl No	*Methods*	*Affected OSI layer*
1	Denial of sleep attack	MAC layer
2	Cross-layer design	MAC and routing layer
3	Energy efficient opportunistic routing	MAC layer
4	Optimal sleep-wake method	MAC layer
5	Sleep deprivation attack	MAC layer
6	Vampire attack	MAC layer

3. Types of Vampire Attacks

Here in this section we present the type of vampire attacks that can target on source routing protocols, such as DSR [9]. In these types of systems, the source node specifies the entire route to a destination within the packet header, so intruders do not make autonomic forwarding decisions, anticipating rather on a route specified by the source. The intermediate node finds itself in the route (specified in the packet header) and transmits the message to the next hop while forwarding a message. The burden is on the source node to ensure that the route is plausible at the time of sending, and also every node in the route is a physical neighbor of the previous route hop. The advantage of this approach is that it requires very little forwarding logic at intermediate nodes, and permits the entire routes to be sender-authenticated using digital signatures, as in Ariadne [10]. There are two important types of vampire attacks: - Carousel attack and Stretch attack.

3.1 Carousel attack

In the Carousel attack, attackers introduce some packet within a route tranquil as a sequence of loops, such that the same node appears in the route of communication many times. This attack increases the routing length and delay very much in the networks and also inadequate by the number of allowable entries in the resource route.

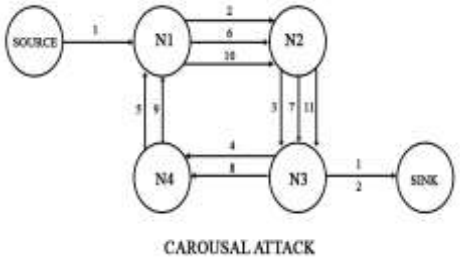

Figure 1: Carousel attack

3.2 Stretch attack

In this type of attack, the malicious node constructs paths to transmit the message to the destination node (which may be an honest one) which is far longer than the optimal path in the topology. An honest node selects the path from source to destination, but the malicious node selects a longer route its affects all nodes in the network. It increases path length of the packet process by number of nodes along the shortest path between the adversary and packet destination.

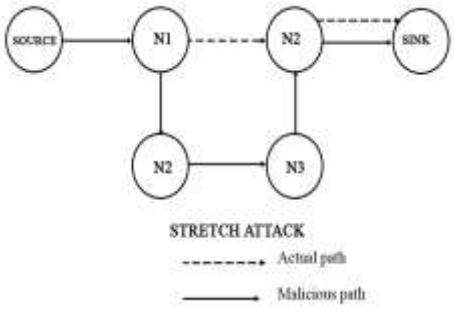

Figure 2: Stretch attack

The carousel attack can be prevented by having forwarding nodes check source routes for loops. This adds extra forwarding logic and thus more overhead, we can expect the gain to be valuable in malicious environments. The ns-2 DSR protocol does implement loop detection [8], but does not use it to check routes in forwarded packets. The source route could be corrected and the packet sent on, when a loop is detected. But one of the attractive features of source routing is that the route can itself be signed by the source [11]. Therefore, it is better to drop the packet, especially considering that the sending node itself is malicious.

The stretch attack is more demanding to prevent. Its success relies on the forwarding node not checking for optimality of the route. We call the no-optimization case strict source routing, since the route is followed exactly as mentioned in the header.

In loose source routing any forwarding node can reroute the packet if it knows a shorter path to the destination or having forwarding nodes check source routes for loops. Unfortunately, this proves to be less efficient and adds extra forwarding logic and thus more overhead than simply keeping global network state at each node, defeating the purpose of source routing [8].

4. Existing system

4.1 Clean-slate secure sensor routing

In this section we tend to show that a clean-slate secure sensing element network routing protocol by Parno, Luk, Gaustad, and Perrig (PLGP) [2] will be changed to resist vampire attacks throughout the packet forwarding section. The initial version of the protocol, although designed for security, is prone to vampire attacks.

PLGP consists of a topology discovery section, followed by a packet forwarding section. Throughout topology discovery section each node should announce its presence by broadcasting a certificate of identity, together with its public key brought up as node ID, we are going to store the neighbor relationship among nodes as tree. Every node starts as its own cluster of size 1, with a virtual address 0. Nodes that catch presence broadcasts form teams with their neighbors. Once 2 individual nodes (each with an initial address 0) type a gaggle of size 2, every cluster member prep ends the cluster address to their own address, e.g., node 0 in cluster 0 becomes 0.0, node 0 in cluster 1 becomes 1.0 and shortly each node at intervals {a cluster|a gaggle|a bunch} can end up with a next-hop path to each different group, as in distance vector. By the top of topology discovery, every node learns each different node's virtual address, and public key.

During the forwarding section, all selections area unit created severally by every node, receiving a packet, a node determines consecutive hop by finding the foremost important bit of its address that differs from the message originator's address, each forwarding event shortens the logical distance to the node, forwards packet p by attaching a non-repayable attestation (signature). These signatures type a chain hooked up to each packet, permitting any node receiving it to validate its path. Each forwarding node verifies the attestation chain to make sure that the packet has never traveled off from its destination. Since all messages are signed by their mastermind, messages from honest nodes cannot be arbitrarily changed by malicious nodes wish to stay undiscovered.

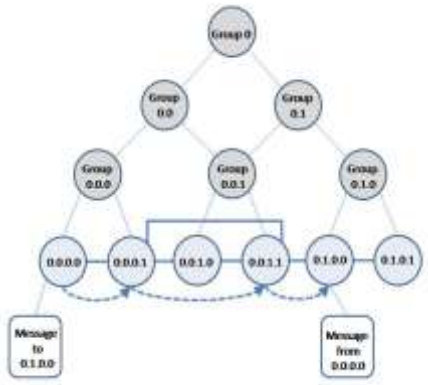

Figure 3: The final address tree for a fully-converged 6-node network

4.2 PLGP in the presence of vampires

In PLGP, forwarding nodes don't recognize what path a packet took, permitting adversaries to divert packets to any part of the network, although that space is logically additional away from the destination than the malicious node. This makes PLGP susceptible to vampire attacks. Contemplate for example the directional antenna attack [10]: a receiving honest node could also be farther removed from the packet destination than the malicious forwarding node, however the honest node has no way to tell that the packet it simply received is moving away from the destination; the sole info obtainable to the honest node is its own address and therefore the packet destination address, however not the address of the previous hop (who will lie). Thus, the vampire will move a packet away from its destination while not being detected. The situation is worse if the packet returns to the vampire within the process of being forwarded it will currently be rerouted once more, inflicting one thing almost like the carousel attack. Recall that the harm from the carousel attack is delimited by the utmost length of the supply route, however in PLGP the individual faces no such limitation, that the packet will cycle indefinitely. Nodes could sacrifice some native storage to retain a record of recent p packets to stop this attack from being dispensed repeatedly with an equivalent packet.

5. Proposed Methodology: Security Against Vampire Attacks

The forwarding phase of PLGP is modified to provably avoid the above mentioned attacks. First we introduce the no backtracking property, satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space. More formally:

Definition 1*: No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network. (Maliciously induced route stretch is bounded to a factor of 1.)*

If a network satisfies this property, that network is resistant to vampire attacks. i.e., no-backtracking implies vampire resistance. PLGP protocol does not satisfy no-backtracking.

The proposed system concentrates on a secure data transmission from the adversary nodes in the sensor network. In order to build a secure network, the network should be an extinct to adversary nodes. So we implement Intrusion Detection System (IDS) in the network. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports. Here we are using Network-based IDSs which uses the network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services.

We implemented a 50 node network topology using NS-2 simulation in that 8 nodes are IDS nodes that continuously monitors the nodes and reports the malicious activities in the network if exists any. The number of nodes monitored by each IDS node depends on the application of the system. In our system each IDS node monitors 6 nodes that is it looks like a cluster with 7 nodes.

IDS provides authentication to the system by using public key cryptosystem. There exists a key-server in the system which distributes the public key to all the nodes in the system which is a randomly generated number. The IDS node distributes the ID-based key to its neighboring nodes which is obtained by using a random function. The nodes after receiving the ID-based key it shows its acceptance by sending an

acknowledgment message signed (attested) by itself. Each node after receiving the message it signs with its own key so that a malicious node cannot falsely claim to be sender of the message. The IDS keeps on monitoring the network and eliminates the attacker if any exist in the network by verifying with the attestation key. When IDS receives any request packet from any node, it calculates the shortest path between the sender and destination and it checks i)the attestation of packet i.e. source and destination address and signature chain and ii) is the node logically closer to the destination than the previous node in the chain. This way IDS can enforce the forward progress of a packet, then IDS transmits the next closest hop IP address and port number in the shortest path to the requested node if the attestation were valid otherwise it discards the packet at the node itself to mitigate the vampire attacks.

6. Results

The proposed system is implemented using NS-2. For this we are using ns allinone 2.35. NS-2 is mainly used for the simulation purposes where we can configure all the protocols such as AODV etc. and simulate the project. Here 50 nodes are considered to form the system. The nodes are configured. The nodes will find its neighbors that are nodes within its transmission range.

The performance analysis of the proposed method using network based intrusion detection system can be clearly understood using the graphs shown below.

Figure 4 illustrates the packet delivery ratio of the proposed system which is shown below.

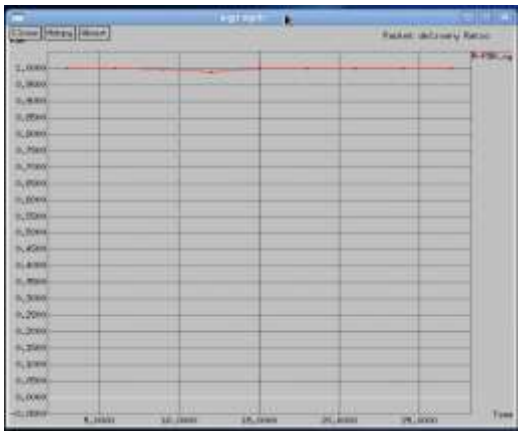

Figure 4: Packet delivery ratio

Figure 5 shows the packet drop in the implementation of the proposed system. From the graph we can clearly conclude that the packet drop is high in the presence of attack.

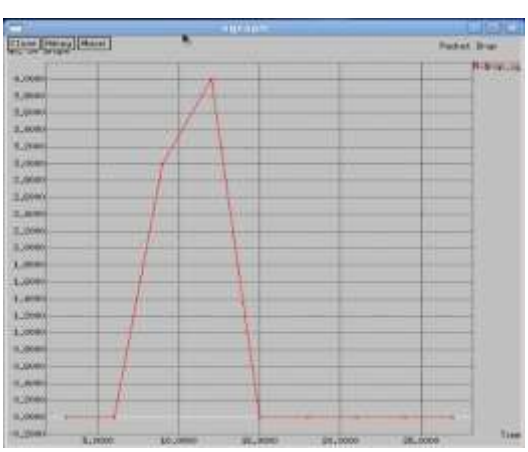

Figure 5: Packet drop of the system

Figure 6 shows the throughput of the system. From the figure we can clearly understand that the throughput is low in the presence of attacker but is high and nearly constant after the implementation of IDS in the network.

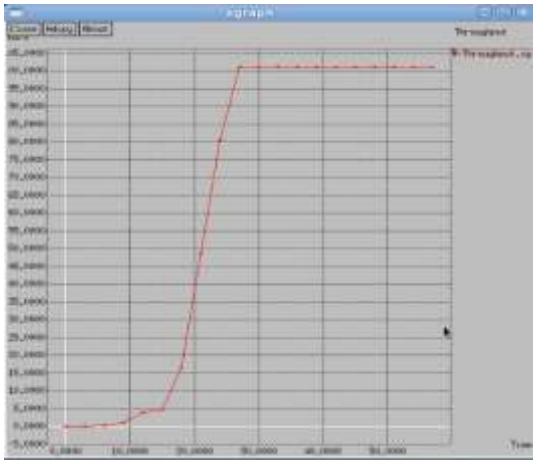

Figure 6: Throughput of the system

7. Conclusion

The proposed technique in this paper, address the properties of routing protocol attacks in the wireless ad hoc networks. In order to overcome the vampire or malicious attacks in WSN, the information transmission is carried in the trusted path of the networks. Our proposed technique addresses the vampire attacks in the wireless sensor networks when compared to the existing approaches. The two types of vampire attacks namely: - the Carousel attack where attackers introduce some packet within a route tranquil as a sequence of loops, such that the same node appears in the route of communication many times and the Stretch attack, where attackers construct falsely long routes, potentially traversing every node in the network, leads the entire networks into collapse, total energy consumption level increases, and allocates long routing path and so on. In this paper, we implement new technique called IDS to detect the misbehavior nodes in the wireless sensor networks.

References

[1] A. Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54–62, 2002.

[2] Ranjitha. R and Sivaraman. P, "Secure wireless ad-hoc sensor network from vampire attack using M-DSDV", IJIRCCE, Vol. 2, Issue 5, May 2014.

[3] Michael Brownfield,Yatharth Gupta, "Wireless Sensor Network Denial of Sleep Attack", Proceedings of 2005 IEEE workshop on information assurance,June 2005.

[4] Jing Deng, Richard Han, Shivakanth mishra, "INSENS: Intrusion Tolerant routing in Wireless Sensor Networks", University of Colorado,Department of computer science Technical report,June 2006 .

[5] Fatma Bouabdullah, Nizar Bouabdullah,Raouf Bouabdullah "Cross-layer Design for Energy Conservation in Wireless Sensor Networks", IEEE GLOBECOM 2008,New Orleans,USA,December 2008.

[6] Xufei Mao,Shaojie Tang, Xiahua Xu, "Energy efficient Oppurtunistic Routing in Wireless Sensor Networks", IEEE transactions on parallel and distributed systems, VOL. 12, NO. 2, February 2011

[7] Tapaliana Bhattasali,Rituparna Chaki,Sugata Sanyal "Sleep Deprivation Attack Detection in Wireless Sensor Networks", International journal of computer applications(0975-8887)vol 40- No: 15,February 2012.

[8] Eugene Y. Vasserman, Nicholas Hopper, " Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE transactions on mobile computing, VOL. 12, NO. 2, February 2013.

[9] D. B. J. D. A. Maltz and J. Broch,"Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks," Computer Science Department Carnegie Mellon University Pittsburgh, PA, pp. 15213–3891, 2001.

[10] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Wireless networks, vol. 11, no. 1-2, pp. 21–38, 2005.

[11] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on, pp. 56–73, IEEE, 2000.

[12] K.Premkumar and Anurag Kumar, "Optimal sleep-wake scheduling for quickest intrusion detection using sensor networks ", IEEE explore, February, 2008.

[13] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure sensor network routing: A clean-slate approach," in Proceedings of the 2006 ACM CoNEXT conference, p. 11, ACM, 2006.

[14] Pushpalata D. Chandore, Devendra Vatsa, and Nitesh Rastogi, "Protection from vampire attacks on routing protocol", International Journal Of Engineering And Computer Science Volume 3 Issue 5, May 2014, Page No. 5801-5806.

[15] Sureka.N and Prof. S. Chandra Sekaran, "Securable routing and elimination of adversary attack from manet", IJIRCCE, Vol.2, Special Issue 1, March 2014.