IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 2, Ver. IV (Mar-Apr. 2016), PP 67-80
www.iosrjournals.org

Network Layer Attacks: Analysis & Solutions, A Survey

Shruthi N[1], C K Vinay[2]
[1]*APS College Of Engineering, Assistant Professor, Department Of Electronics & Communication Bangalore, INDIA*
[2]*Hewlett Packard, SVC Info Developer II, Bangalore, INDIA*

Abstract *- An ever-existing concern is the lack of security due to the very fact that the technology is wireless and is vulnerable to security threats & attacks. Also, among the wide-spread characteristics of a CR, self-organized security management is one of prime considerations. Each layer in cognitive radios is susceptible to widespread threats and security attacks. The scope of this paper reveals a detailed tabulation of the possible security threats/attacks faced by cognitive radios & cognitive radio networks in the Network layer, along with the current state-of-the-art to detect the corresponding attacks and discuss the possible countermeasures for the same. The paper makes an attempt to effectively survey the existing detection techniques as well as counter measures relevant to Network layer attacks.*

Index Terms: *Network Layer Attacks-Threats, network security, countermeasures, routing, cognitive radio networks (CRNs), protocols.*

I. Introduction

The conceptualization of Computer & Network security started way back in the 1930's and even today countering security breaches are on high priority for all leading organizations. Network security has been gaining attention with the expansion of internet. Modern computer networks are characterized by mainly layered architectures and flexibility that these architectures provide should be prevented from posing as a security breach.

This paper mainly concentrates on the Network Layer attacks and threats, their possible counter measures and formulation of the future of Network security and hence focus will mainly be on the network layer. It becomes vital for a network analyst to understand the security concerns of a general WSN prior to the NL security. WSNs are more prone to attacks due to wireless transmission. Nodes may also deploy on unsafe, unpredictable hostile environments. It is evident that the Network Layer (NL) is responsible for routing, flow control and quality-oriented data handling and forwarding and hence all this calls for an extremely secure Network Layer. Threats or an attack of any kind to this layer is a disruption to the above mentioned services rendered by the NL. In additional to security attacks, the NL also encounters design issues like Store-and-forward packet switching, Services provided to transport layer, implementation of connectionless and connection-oriented service and comparison of virtual-circuit and datagram networks.

The network layer accommodates a stream of subnetwork technologies and interconnection strategies, providing a common service interface to the transport layer. Standard network layer protocols available are ISO/IEC 8880, 8348 and 8648. The first standard gives an overview of the network layer whereas 8348 and 8648 define the layer's internal organization and network service. Another recent addition is ISO/IEC 11577 describing the Network Layer Security Protocol (NLSP).

II. Types Of Network Layer Attacks

The Network Layer is responsible for intra-network operation, different type addressing routing information through the sensor network, finding the most efficient path for the packet to travel on its way to a destination. It handles the routing of the data and forwarding from node to base station and vice versa. The network layer is present just above the link layer in the protocol stack and holds the responsibility of performing routing, flow control and ensuring quality of service (QoS). Routing is the selection of communication path between source and destination enabling end-to-end packet delivery. However, every node in the network maintains routing and neighbouring node information.

Routing attacks can be categorized as routing disruption attacks and resource consumption attacks. Network endo-parasite attack increases the interference at heavily loaded high priority channels. Nodes conceal change information from neighbours resulting in internal parasites. These poor channels induce interference and deteriorate performance. The different attacks have been discussed below in detail.

1) Sinkhole Attacks

As multi-hop routing is mainly used by CRN's, attacking nodes find it easy to attack legitimate nodes in hops [2]. According to the sinkhole attack scenario, attacker will project himself as the best route provider to a specific destination, which is usually a low latency route. When other legitimate nodes send data packets in this false route, the attacker either misuses or discards that packet from the network. Attacker can use that packet to perform many attacks such as eavesdropping, changing information from packet and resending it etc; the attacker can perform selective forwarding packets from select nodes.

Possible thoughts of solution to sinkhole attacks include geo-routing protocols like AODV and DSR [3], authentication by the fusion center and redundancy checks. In these routing protocols, the source node wanting to transmit a message has to obtain a security metric. Only if the metric is satisfied, the message will be forwarded to the next intermediate node. On receiving this message, destination sends a route reply to sender through the same intermediate nodes that had participated in the route request message earlier. These route request and reply messages contain a ciphered key that prevents any malicious node from decrypting the messages. Therefore, even if the attacker generates messages with changed security levels, the legitimate nodes will drop these packets since they do not contain the correct ciphered key generated by the base station. The multi-hop nature of sensor networks along with specialised communication patterns make them more susceptible to these attacks.

Few other countermeasure principles include Routing Access Restriction (Multipath Routing & authentication) and False Routing Information Detection [4]. A typical way to resist sinkhole attacks has been proposed by authors of [5] as well. The authors of [6] have surveyed and compiled details of a few countermeasures for sinkholes. They include Data Consistency & Network Flow Information Approach, Hop Count Monitoring Scheme, RSSI Based Scheme, Monitoring node's CPU usage, Mobile Agent Based Approach, Using Message Digest Algorithm.

2) Sybil Attacks

A malicious node presents multiple identities to the network to create confusion to nodes, due to which an adversary seems to be present in multiple positions/locations at the same time. Such attacks are the "Sybil Attacks." In a spectrum wherein all nodes participate cooperatively in decision – making, the attacker can send wrong sensing information which lead to wrong sensing decision and hence let the PUs channels unused wrong information can propagate through the entire node chain. Node's identity validation technique is used to mitigate this attack wherein there are two ways of validation used which are direct and indirect validation. In direct validation, each node tests directly the valid identity of other. On the other hand, in indirect validation, other verified nodes can validate other nodes. All participating nodes must have validated identities by possessing a unique key shared with only the base station. Authors of [7] propose a cryptography based algorithm for handling Sybil attacks.

Other detection techniques have also been discussed.

(a) Usage of directional antennae: Even though this method is not very efficient in attack detection, it is sometimes used to check whether the messages have arrived from forged neighbours.

(b) Signal Power Matching: Propagation model is implemented in which the received signal power from a sending node is matched with its claimed position to calculate the node position. The node will be termed as "Sybil" node when there arises a mismatch between the claimed and calculated values. This method is not suitable for small-scale attacks.

(c) Resource Testing: Each node irrespective of whether true/malicious node is tested for its computational resources. A malicious node having more resources may mislead a decision. However, Radio Resource Testing assumes that every node has only one radio that can only send/receive one channel at a time. But, multiple radio devices cannot be accessed simultaneously and this is a disadvantage.

(d) Localization of nodes: This method is based on finding the physical location of nodes and comparing it with the vehicle's position is to discover the attack. This solution is the geometric method using GPS data.

(e) Public Key Cryptography: Signatures combined with digital certificates and asymmetric cryptography is used. Unique certificates are issued by the CA, CA tracks all the issued certificates.

(f) **Timestamp Series**: Detection based on roadside support unit (RSU) wherein a vehicle node gets a timestamp every time it passes through a RSU. Sybil attack can be detected if multiple traffic messages contain very similar series of timestamps.

Authors of [8] discuss the existence of a Sybil Detection Game (SDG) with integration of reputation mechanism. Also, in [8], a signalling game model is revealed in which the Sybil node reveals its identities if and only if detective offers reward. A RSS-based Sybil detection scheme has also been proposed. This scheme uses the 802.11 protocol without the need for any extra hardware unlike other RSS based schemes to counter Sybil attacks. The entry and exit behaviour of legitimate nodes and Sybil nodes is analysed first. A threshold that distinguishes between the legitimate and Sybil identities based on nodes' entry and exit behaviour is identified. Detection threshold is tuned by incorporating the RSS data fluctuation. Other Sybil countermeasures have been surveyed in the same paper as groundwork. A defense mechanism to counter Sybil attacks in MANETs using the (Associativity Based Routing (ABR) protocol has been proposed in [9] to detect the attacker. An extended concept is implemented in [10] using the Q-Learning Based ABR (QABR) protocol to detect the Sybil attacker.

3) Hello Flood Attacks

In this attack, the attacker try's to broadcast a message (say "hello") to all nodes in the network to convince that it is the neighbour node of the victim node which just a few hops away. The victim node may also get convinced due to the strength of the signal sent. But sufficient amount of power is needed to be used to convince each node that attacking node is its neighbour. Another perspective is that the nodes forward their packet destined to a particular node through this attacking node with regular signal power level, but the messages may be lost due to the far distance of the attacking node/ forwarding node, thereby resulting in packet loss.

These attacks can be avoided by verifying the bi-directionality of a link before taking action based on the information received over that link. The Needham-Schroeder verification protocol [11] is one of its kind used to target the HELLO flood attacks. In fact, this attack can be prevented all together if the base station limits the number of verified neighbours.

4) Page Hole Attack

Page Hole Attacks can be categorized as Black hole attacks, Grey hole attacks and Worm hole attacks. The node which pretends is referred to be a Hole.

The Black hole attack is that in which the malicious node requests packets from neighbour nodes and drops all of them. The black hole attack first positions a node in range of the sink. The false node advertises itself as the shortest path facilitator and attracts the entire data traffic. However, unauthorized nodes can be identified by checking replies from authorized nodes. In MANETs, black holes are countered with the help of the AODV (Ad hoc On Demand Distance Vector) protocol. It is a pure reactive protocol and it incorporates the features of both DSDV (Destination sequenced Distance vector routing) and DSR (Dynamic Source routing protocol). An up gradation of AODV is the Improved AODV with extended security and other additional features like Path Accumulation, Multipath routing and Hybrid routing type [12]. A trust based approach for mitigating black hole attack in AODV protocol has been proposed. The method monitors the data packets being transmitted to neighbouring node in promiscuous mode and assigns a trust value to its neighbour dynamically and periodically. Future communications with neighbouring nodes are based on this trust value [13].

Many other trust based approaches have been proposed prior to [13]. TAODV protocol [14] calculates trust value based on others opinion (may be malicious nodes sometimes). It uses an additional overhead – digital signature. Watchdog concept was introduced by authors of [15]. Watch dog calculates a trust value after listening to neighbouring nodes transmission. Based on this value, trust value on the neighbour will be increased or decreased dynamically. This method is implemented only on the DSR protocol. Multiple paths to destination is next concept adopted and demonstrated in [16]. This solution fails, if more than one path is not available. Also, the solution may bring unwanted delays to the network by waiting for multiple RREP (Route Reply) packets. An Artificial Immune System (AIS) has been discussed in [17] to detect a misbehaving node in MANETs. This system itself requires a protected environment at beginning for learning in order to adapt to the real time environment. Authors in [18] have proposed another solution to black hole attacks taking into consideration RREP messages received and RREQ (Route Request) messages sent. The concept is that malicious node will send RREP messages with extremely higher sequence number, therefore the average sequence number is found out. A similar effort has been made in [19] where black hole attacks are detected based on destination sequence number. This solution challenges detection of multiple attackers simultaneously and promises larger thresholds. The first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the Route Request Table (RRT). The first destination sequence number is then compared with the source node sequence number. Node will be termed "malicious" and removed from the RRT if there exists large differences between the RRT values.

TOGBAD [20] is a black hole detection system looks at the number of neighbours a node claims to have and the actual number of neighbours according to a topology graph. This was mainly for the OLSR proactive routing protocol. Another detection scheme [21] was developed for AODV in which, on receiving a reply, the receiver node initiates a judgement process about the replier. A detection method is proposed by [22] authors sequence number checking of the RREP packets forms the basis. The authors of [23] have surveyed about few black hole attack detection methods like the neighbourhood based method along with a routing recovery protocol, a watch-dog based collaborative method, Aggregate Signature algorithm for tracing packet dropping nodes. A feasible DSR-based solution called the DBA-DSR scheme has been proposed by the authors of [24] to mitigate black hole attacks in MANETs. This scheme can be further be improved to handle cooperative black hole attacks.

Jellyfish attack is a type of Black hole attack in which data gets compromised but till certain time only. These can increase the capacity of ad hoc networks as they will starve all multi-hop flows. These attacks target TCP traffic [25].

Grey hole attack is that attack in which the attacker node selectively drops the packets. It is a refined version of a black hole attack wherein a malicious node drops only selected data packets and forwards the rest depending upon the source or destination of packets. Trust based mechanisms cannot solve these attacks. The authors of [26] propose a Grey hole detection scheme for DSR protocol. The mechanism is a combination of aggregated signature algorithm for the node to produce evidence on forwarding packets, checkup algorithm to check if nodes are dropped or not and a diagnostic algorithm to trace malicious nodes. A slight modification of the above scheme along with a Distributed Certificate Authority (DCA) has been discussed in [27]. A detection scheme for AODV protocol [28] requires all nodes to maintain their neighbours' data forwarding information.

The authors of [29] have proposed an adaptive black and grey hole detection algorithm based on cross-layer design. This algorithm is said to be saving the system resources since extra control packets are not being sent. Nital et. al [30] has put forth an improvement over the AODV protocol against the black hole attacks. The proposal highlights a marginal rise in average end-to-end delay and improvement in packet delivery.

Worm hole attack is that in which there will be two malicious nodes in which there will be private connection between two pairs. If the end point of Worm hole is relatively far from the base station, most nodes in local network area will try to use attacker for forwarding. These low latency links between two nodes help transfer and replay messages. Wormhole attacks are divided into two categories, namely 'hidden' and 'exposed' attacks, depending on whether malicious nodes put their identity into packet headers when tunnelling and replaying packets [31]. An attacker close to the base station can create well positioned wormholes that convince nodes that they are valid nodes which are just a few hops away. Even though these wormholes are not very dangerous as a standalone entity, when coupled with selective forwarding, they are a threat to any communication network. The hard bottlenecks in wormholes are that they use invisible channels and hard to trace routes. Wormhole attacks are considered to be the most sophisticated attacks in MANETs. Few wormhole detection methods have been proposed in [32, 33]. Geographic (location-based) routing protocols are resistant to these attacks because messages are routed towards the physical location of the base station. Another solution would be to provide tight time synchronization which is often not feasible since it requires the original protocol design. Other solutions include Authentication, probing, providing anonymous IDs of neighbouring nodes. Therefore, any wormhole trying to convince two distant CR nodes that they are true neighbours will fail when they check their list of anonymous IDs and distances. Authors of [34] propose a GPS based solution to counter wormhole attacks, wherein nodes have been broadly categorised into GPS and non-GPS nodes. Wormhole Attack Prevention (WAP) [35], using Neighbour Node Monitoring (NNM) discusses hidden as well as exposed attacks. An encoding based multipath routing solution has been proposed in [36] where initial message is divided into chunks and characteristic of existence of multiple paths between nodes in an ad hoc network is exploited to increase robustness against attacks. [37] proposes a solution where time taken by packet to come back from 1-hop and 2-hop neighbours is the determining criteria to handle attacks. One of the most recent papers [38] has proposed an algorithm DAWN typically suited for distributed WNs. The algorithm does not rely on any location information, global synchronization assumptions or special hardware/middleware. It is only based on the local information that can be obtained from regular network coding protocols, and thus the overhead of our algorithms is tolerable. It aims at detecting and localizing the wormholes. Few wormhole detection mechanisms are discussed below [39]:

(a) Distance-bounding/Consistency-based Approach – The concept involves two communicating sensor nodes to estimate the actual distance between them. This technique is based on message travelling time information, directional antennas or geographical information and may not be practically considered for few networks since specialized hardware is demanded. Some of the solutions based on this approach are:

(i) **Message Travelling Time Information Solutions** - Message travelling time information is usually expressed in terms of round trip time (RTT). This RTT is used to determine the distance between nodes and decide whether the calculated distance is within the maximum possible communication range.

(ii) Special Hardware-based Solutions - Directional antennas are employed for access restriction and neighbour discovery. A protocol named "SECTOR" was implemented wherein distance between two sensor nodes can be measured accurately based on the speed of data transmitted between them. The MADB (Mutual Authentication with Distance bounding) protocol enables the nodes to determine their mutual distance at the time of encounter. Another protocol based on one-bit challenge and time of flight is also considered as a solution provided it has the support of a non-delay hardware.

(iv) Geographical Information-based Solutions - Authentication is applied to each data packet to introduce the concept of geographical and temporal packet leashes for detecting wormholes [40]. The maximum difference between any two nodes' clocks is bounded by a predetermined threshold known to all the nodes used to determine the packet expiration time. If the receiving time of a packet exceeds the packet expiration time, the packet is discarded.

(v) Synchronized Clock-based Solutions – These solutions assume that all sensor nodes in the network are tightly synchronized and each data packet includes the time at which it is sent out. When a data packet is received, the receiver node compares the receiving time with the time at which the packet is sent out. As the receiver node has the knowledge of transmission distance and consumed time, it is able to detect how far the packet has travelled. If the transmission distance exceeds the maximum allowed travel distance, the network is probably under a wormhole attack.

(vi) Multi-dimensional Scaling-Visualization-based Solutions - based on the observation that the network with malicious nodes has different visualization from that with normal nodes. Multi-dimensional scaling is used to construct the layout of the sensor nodes which can be reconstructed and visualized. If wormhole attackers exist, the shape of the constructed network layout will show some bent/distorted features and detects the wormhole by visualizing the anomalies introduced by the attack.

(vii) Trust-based Solutions - Sensor nodes can monitor the behavior of their neighbouring nodes and rate them based on the trust information and choose the most trustworthy, efficient path.

(viii) Localization-based Solutions – These may include a distance consistency- based secure location approach or a graph theoretical method to prevent wormhole attacks.

(ix)Secure Neighbour Discovery Approaches - The fundamental mechanism used is local monitoring. The neighbouring list of each node is being built. Later, a collaborative detection strategy for wormholes is used, where a node monitors the traffic going in and out of its neighbours. A sensor node monitors the traffic in and out of its neighbouring nodes and uses a data structure for the first and second hop neighbours.

(x) Connectivity-based Approaches – These are less frequently used since connectivity information is hard to determine in real-time, used only in dense networks [41]. Connectivity information in the connectivity graph. No special hardware or location Information is required.

(xi) Radio Fingerprinting Approaches - The radio signal first is received by the fingerprinting device and then converted to its digital format. The signal transient is then located and its features are extracted. A set of features form a fingerprint that can later be used for device identification. This approach can be implemented on sensor nodes, however, there are many open unsolved loops with regard to the same.

5) Ripple Effect

This is a new type of attack in which the malicious node attempts to provide wrong channel information, so that other nodes will change their channel, and finally entire traffic in network will be disrupted. When the attacker sends strong signals this attack will be more effective since the activities of PU are larger than that of SU thereby disrupting the SU transmissions. When SU's change their channel, energy will be expanded to facilitate for the Spectrum. So this attack is similar to that of primary user emulation and Byzantine attacks. The compromised node can transmit the misleading channel information and force other nodes to adjust their channel assignments. A probable thought of solution is continuous trust management process on SUs.

6) Channel Endo Parasite Attack

A compromised node launches an attack by switching all its interfaces to the channel that is being used by the highest priority link. A serious attack can be easily detected.

7) Network Endo Parasite Attack (NEPA)

Malicious nodes attempt to increase the interference at a heavily loaded high-priority channel. A compromised node launches NEPA by assigning its interfaces the high priority channels but the neighbours are not informed about the change [42]. A probable approach to solve the above mentioned parasitic attacks would be an implementation of an appropriate local spectrum sensing controller and eliminating internal hidden parasite nodes.

8) Homing

In a homing attack, the attacker looks at network traffic to deduce the geographic location of critical nodes, such as cluster heads or neighbours of the base station. The attacker can then physically disable these nodes. As a solution, dummy packets can be used throughout the network to equalize traffic volume and prevent traffic.

9) Node Replication/Clone Attacks

This is an attack where the attacker tries to mount several nodes with the same identity at different places of the existing network. The attacker either captures one node from the network, creates clones of a captured node and mounts in different places of the network else, an attacker generates a false identification of a node, makes a clone out of this node and mounts in different places of the network. These clone nodes may create a black hole, wormhole or leak out secure data as well. If these nodes are not identified attended to, they can induce change in protocol behaviour and affect network security [43].

Detection techniques can be classified as centralized and distributed. In centralized techniques, every node sends its location claim (ID, Location Info) to base station (sink node) through its neighbouring nodes. The base station checks the node IDs and their location. Base station raises an alert if two different locations with same ID are detected. Below are few centralized techniques-based solutions for node replication attacks:

Using Random Key Distribution [44] – Keys follow a pattern according to the random key distribution scheme. Key will be termed as “cloned” if the key exceeds a threshold. SET [45] method wherein network is divided into exclusive subsets. Multiple roots are randomly decided to construct multiple subtrees, and each subset is a node of the subtree. Each subset leader collects member information and forwards it to the root of the subtree. If intersection of all subsets of a subtree is empty, there are no clone nodes in this subtree.

Real time clone detection techniques [46] have been dealt with wherein each sensor considers the neighbourhood information through a superimposed s-disjunct code and computes a fingerprint. A node sending a message also includes the fingerprint in it which the neighbouring nodes can verify.

Cluster head selection-based hierarchical distributed Algorithm LNCA [47] uses a Bloom filter mechanism including network reactions. Compressed Sensing-based Clone Identification (CSI) [48] is proposed for static WSNs. Each node broadcasts a fixed sensed data to its one hop neighbours. Sensor nodes forward and aggregate the received numbers from descendant nodes along the aggregation tree via compressed sensing-based data gathering techniques. Base station receives the aggregated result and recovers the sensed data of the network.

In distributed techniques, detection is performed by locally distributed node sending the location claim not to the base station (sink) but to a randomly selected node called witness node. The category of solutions is as below: Node-to-Network Broadcasting (N2NB) and Deterministic Multicast (DM) protocols [49]. In N2NB, each node floods the entire network with authenticated broadcast to claim its own location instead of its neighbours. In DM, the claimer locally broadcasts its location claim to its neighbours, each neighbour serving as a reporter, and employs a function to map the claimer ID to a witness. Distributed witness-based Detection algorithms Randomized Multicast (RM) and Line Selected Multicast (LSM). RM distributes location claims to a randomly selected set of witness nodes and LSM selects witnesses for a node location and utilizes geometric probability to detect replicated nodes. Group/Generation based detection algorithms [50, 51] by limiting the order of deployment using symmetric polynomial for pair-wise key establishment. RED protocol executed at fixed intervals of time [52, 53]. A random value is shared between all the nodes through base station and later each node broadcasts its claim (ID and location) to its neighbouring nodes. Cell division-based algorithms Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC) [54, 55]. In SDC, each node ID is uniquely mapped to one of the cells in the grid. Each node broadcasts a location claim to its neighbours, each neighbour forwards the location claim with a probability to a unique cell by executing a geographic hash function with the input of node ID. In P-MPC, the location claim is mapped and forwarded to multiple deterministic cells with various probabilities; rest is the same as in SDC.

A polynomial based space-time-related pair-wise key pre-distribution scheme (PSPP-PKPS or just PSPP) for wireless sensor networks [56], which relates the keying material of a node with its deployment time and location. A real time neighbour-based detection scheme (NBDS) involves the implicit verification of a node’s information furnished to its neighbours [57]. A node capture detection scheme [58] wherein the captured sensor nodes are detected by sequential analysis. Memory efficient protocols [59] namely memory efficient multicast with Bloom filters (B-MEM), memory efficient multicast with Bloom filters and Cell Forwarding (BC-MEM), memory efficient multicast with cross forwarding (C-MEM), and memory efficient multicast with cross and cell forwarding (CC-MEM). Active detection protocol in which each node verifies at random a few other nodes in the network [60]. Each node actively tests if 1 k other random nodes are replicated or not; they are scrutinized nodes. A novel clone node detection protocol called randomly directed exploration [61] wherein each node only needs to know its neighbouring nodes. Protocols RAndom WaLk (RAWL) and Table-assisted RAndom WaLk (TRAWL). RAWL starts several random walks randomly in the network for each node, and then selects the passed nodes as the witness nodes of that node [62]. On the other hand, TRAWL adds a trace table at each node to reduce memory cost.

Mechanisms based on intersecting sets [63] called CINORA-Inset and restricted cell two-phase authentication model called CINORA-Hybrid where sensor network is divided into geographical cells similar to the existing cellular network. A note-based randomized and distributed protocol called NRDP, no significant overhead on the resource-constrained sensors [64]. Geographical information of nodes is also not demanded. Group deployment knowledge-based schemes based on the assumption that nodes are deployed in groups [65]. Replica detection is carried out. A distributed protocol that does not need any reliable/trusted entities [66]. A distributed, deterministic approach [67] which includes initialization, witness node discovery phase, and node revocation phase.

10) Selective Forwarding

Here, the adversary chooses a data path of interest. Attackers may choose not to forward certain packets and drop them creating a sort of black hole/vacancy. A variation of this attack is when the adversary only drops packets coming from a specific source whilst reliably forwarding other packets. Such attacks are much harder to detect than black hole attacks. One can implement multiple path routing to control selective forwarding attacks, the probability of selecting a vulnerable route can be reduced. Then, at least one message will travel along a path that is disjoint from the selective forwarding node [68]. Multi path routing can be used in combination with random selection of paths to destination. Braided paths representing paths with no common link or consecutive nodes can also be used ensure that packets are forwarded as they were sent. Base station sets a time limit. If this limit is exceeded and the PU or SU has not received the message, it will inform the BS through another secure node. The BS will then resend the message using that route or another one if needed [69].

11) Alteration, Spoofed and Replay of information

Encryption technique applied to some of the fields of the header message, to avoid communicating some extra bits. One can broadcast authenticated messages by using conventional techniques like packet overhead or the digital signatures. For authenticated broadcast and flooding, an efficient protocol i.e. TESLA and symmetric key cryptography are used. Tiny Sec & SNEP schemes focus on providing message authenticity, integrity and confidentiality, Semantic security, Data authentication, Replay protection.

12) Misdirection Internet SMURF Attacks

If it is observed that a node’s network link is flooded without any valuable information, then for sometime the victim node can be scheduled to sleep.

13) Acknowledgement Spoofing

Protocols affected by acknowledgment spoofing are those which choose their next hops based on reliability issues [68]. The attacker spoofs acknowledgement convincing the sender that an actually weak link may turn out to be strong/ alive one. Due to this misconception, some valid data packets may be lost when travelling along such links. The most obvious solution to this problem would be authentication via encryption of all sent packets and also packet headers. All proposed solutions only aim at the fact that even though every node possesses the ability to verify the identity of the base station, nodes must not spoof messages from the base station.

14) Rushing

This attack can be carried out against on-demand routing protocols that use duplicate suppression in their operations. Conceptually, each intermediate node processes only the first received route request packets and rejects any duplicate packets that arrive later, to reduce the route discovery overhead. Rushing node exploits this mechanism by quickly disseminating route request packets in order to be included in the discovered routes [70]. Rushing attack can be performed in the following ways: by transmitting at a higher wireless transmission power level, by ignoring delays at MAC or routing layers, by keeping other nodes’ transmission queues full or by using a wormhole tunnel [71]. Rushing attacks are said to be countered using Secure Routing Protocol (SRP) [72] which was examined and verified to be a good solution by Rawat et al. in [73].

III. Network Layer Detection & Solution Schemes

To save the power of sensor so as to increase the life of sensor, network layer use SMECN (Small Minimum Energy Communication Network) and LEACH (Low Energy Adaptive Clustering Hierarchy) protocol .

Sybil attacks in the link layer can be successfully detected using several algorithms. The authors in [74] propose an algorithm based on exploitation of spatial variability of radio channels in scattered environments. An algorithm based on the ratios of received signal strength indicators (RSSI) has been presented in [75]. If these ratios are very close to the ratios computed when a packet with a different identity is used, the corresponding transmitter is a proven Sybil attacker. A detection mechanism can always bank upon the fact that every Sybil attacker has a common set of neighbours since they are created by the same adversary. Information collected from all neighbours is used to detect the Sybil attack. One such algorithm is mentioned in [76].

There exist both Preventive as well as Reactive mechanisms. In preventive mechanism, the conventional approaches such as authentication, access control, encryption and digital signature are used to defend attacks. Reactive mechanism uses schemes like Intrusion Detection Systems (IDS) to detect misuse and anomalies and cooperation enforcement mechanisms to reduce selfish node behaviour. IDS systems can be classified [77] as anomaly-based intrusion detection (ABID) or behaviour-based intrusion detection, misuse detection or knowledge-based intrusion detection (KBID); and specification-based intrusion detection (SBID). ABID systems are those in which the model of normal behaviour of the network is extracted, and then this model is compared with the current behaviour of the network to detect intrusion in the network. KBID systems use a database of signatures or patterns of well-known attacks. SBID systems explicitly define specifications as a set of constraints and use them to monitor the routing protocol operations or network layer operations to detect attacks in the network. The first security scheme provided by IEEE 802.11 standards for WLAN is Wired Equivalent Privacy (WEP). It is evident that WEP is prone to message privacy and message integrity attacks and probabilistic cipher key recovery attacks. Few of the disadvantages of WEP like lack of Key Management and combined use of non-cryptographic integrity algorithm, CRC 32 with stream chipper increases security risks [78]. The authors of [79] have surveyed few security protocols for different Network Layer Attacks. The SAR (Secure-Aware Ad Hoc Routing protocol) uses encryption and decryption and a common key. This method demands more number of individual keys when there is a rise in the number of security levels. SEAD (Secure Efficient Ad Hoc Distance Vector Routing protocol) mainly designed for DSDV (Destination-Sequenced Distance Vector) can overcome DoS, all types of routing attacks and resource consumption attacks. SEAD avoids routing loops. ARAN (Authenticated Routing for Ad Hoc Networks) is based on cryptographic certificates which overcome all types of attacks in the network layer. A Collaborative Reputation Mechanism (CORE) enforces node cooperation in Mobile Ad hoc Networks and mainly used for selfishness detection in the MANETS through node co operation mechanism. CONFIDENT Protocol: Cooperation Of Nodes--Fairness In Distributed Ad hoc Networks provides trust based routing security in MANETS. Timed efficient stream loss tolerant authentication (TESLA) protocol counters attacks in MANETs. WATCHERS (Watching for Anomalies in Transit Conservation is a protocol designed to detect disruptive routers in fixed networks through analysis of the number of packets entering and exiting a router. SCAN (self-organized network layer security in mobile ad hoc networks) balances packet delivery. Detection, Prevention and Reactive AODV (DPRAODV) is to counter black hole attacks. MEPA method proposes a minimum exposed path to attacks. AODV-WADR (Wormhole Attack Detection Reaction) proposes a method to avoid the attack using Diffie - Hellman key exchange algorithm. SECTOR uses the distance bounding algorithm to detect the wormhole attacks. MDSVOW uses multidimensional scaling to reconstruct the network and to detect worm holes. WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks without using any specialized hardware wormholes can be detected and isolated within the route discovery phase. ARIADNE is a well-known secure on-demand ad hoc network routing protocol to avoid routing attacks and DoS attacks.

IV. Solutions/Algorithms To Combat NL Attacks - Tabulation

The possible security approaches for attacks in different layers can be generalized as use of spread spectrum techniques and error correcting codes, use of MAC layer admission control mechanism, authentication and cryptography algorithms.

Threat/Attack	**Concepts of Counter Measures/Strategies**	**Performance Algorithms/ Work Reference/Author Name**
Sinkhole attack (routing attack)	➢ Use of geo-routing protocols ➢ Redundancy checks ➢ Authentication by fusion center ➢ Ciphered route request and reply messages ➢ Routing Access Restriction ➢ False Routing Information Detection ➢ Detection on Mint Route ➢ Probabilistic next hop selection ➢ Data Consistency & Network Flow Information Approach, Hop Count Monitoring Scheme, RSSI Based Scheme, Monitoring node's CPU usage, Mobile Agent Based Approach, Using Message Digest Algorithm	➢ Mahmoud Khasawneh et al. **[3]** ➢ Karlof C et al. **[4]** ➢ Fabrice Le Fessant et al. **[5]** ➢ Shahriar Mohammadi et al. **[80]** ➢ Vinay Soni et al. **[6]**
Sybil attacks	➢ To ensure that every node shares a unique symmetric key with a trusted base station since prevention at the link layer does not allow the attack to pass on to the Network layer. ➢ Authentication, monitoring ➢ Usage of techniques like SybilGuard, SybilShield, SybilLimit, SybilDefender, SyMon ➢ Use anonymous Ids frequently changed and possess	➢ Heena Singh et al. [82] ➢ L. Xiao et al. [74] ➢ M. Demirbas et al. [75] ➢ K. SSu et al. [76] ➢ Hanen Idoudi et al. [69] ➢ Mahmoud Khasawneh et al. [3] ➢ Majid Meghdadia et al.

	authentication certificates ➢ Node's identity verification – direct or indirect ➢ Multifactor authentication scheme & Radio Fingerprint ➢ Detection techniques like use of directional antennae, propagation model, resource testing, node localization, public key cryptography and timestamp. ➢ SDG (Sybil Detection Game) ➢ Auto defense mechanism using ABR (Associativity Based Routing) protocol ➢ Auto defense mechanism using QABR (Q-Learning Based ABR) protocol	[31] ➢ Mina Rahbari et al. [7] ➢ Xiaojuan Liao et al. [8] ➢ Sowmya P et al. [9] ➢ Anitha V et al. [10]
HELLO flood (routing attack)	➢ Verifying bi-directionality of a link based on the information received over that link before taking action. ➢ Needham-Schroeder verification protocol ➢ Authentication, packet leashes by geographical and temporal info. ➢ Use of authenticated broadcast protocols ➢ Enforcement of certificates and authentication. ➢ Replacement of routing protocols that use link layer acknowledgments with more secure protocols. ➢ Restricting number of node's neighbours ➢ Link layer encryption and global shared key mechanisms	➢ Heena Singh et al.[82] ➢ T.Kavitha et al. [83] ➢ Adrian Perrig et al. [11] ➢ Hanen Idoudi et al. [69] ➢ Virendra Pal Singh et al. [84] ➢ Shahriar Mohammadi et al. [80]
Black hole Attack:	➢ Identification of unauthorized nodes by checking replies from authorized nodes. ➢ AODV and Improved AODV protocols like AODVSEC (Security Extension) ➢ Trust based Collaborative approach/ Algorithms ➢ A feasible DSR-based solution called the DBA-DSR scheme ➢ TOGBAD based on topology graph for OLSR protocol ➢ For OLSR protocol ➢ Based on sequence checking number ➢ Neighbourhood based method along with a routing recovery protocol, a watch-dog based collaborative method, Aggregate Signature algorithm for tracing packet dropping nodes ➢ Adaptive algorithm based on cross-layer design	➢ Heena Singh et al. [81] ➢ Jaspal Kumar et al. [12] ➢ Fidel Thachil et al. [13] ➢ [14] ➢ Seungjin Park et al. [15] ➢ Y.C. Hu et al. [16] ➢ Slavisa Sarafijanovic et al. [17] ➢ Satoshi Kurosawa et al. [18] ➢ Pooja Jaiswal et al. [19] ➢ Isaac Woungang et al. [24] ➢ E.Padilla et al. [20] ➢ M. Medadian et al. [21] ➢ X.Y. Zhang et al. [22]
Grey Hole Attack	➢ For DSR protocol ➢ Modification of the above along with DCA ➢ For AODV protocol with data forwarding information of node ➢ Adaptive algorithm based on cross-layer design	➢ G.Xiaopeng et al. [26] ➢ C. Wei et al. [27] ➢ J.Sen et al. [28] ➢ Disha G. Kariya et al. [29]
Wormhole attacks	➢ Use of location-based routing protocols wherein the node is aware of the hop distance from the sink. ➢ Usage of geographically shortest or very tight time synchronization among the nodes, which is normally infeasible in practical environments ➢ Authentication, probing ➢ Providing nodes with anonymous IDs of neighbouring nodes in encrypted form. ➢ Use of Distance-bounding/Consistency-based Approach, Synchronized Clock-based Solutions, Multi-dimensional Scaling-Visualization-based Solutions, Trust-based Solutions, Localization-based Solutions, Secure Neighbour Discovery Approaches, Connectivity-based Approaches, Radio Fingerprinting Approaches ➢ DAWN (Distributed detection Algorithm) for distributed WNs ➢ Clustering and Digital Signatures ➢ Use of OLSR and MAD protocols ➢ Usage of directional antennae	➢ Heena Singh et al. [81] ➢ T.Kavitha et al. [83] ➢ Hanen Idoudi et al.[69] ➢ Majid Meghdadia et al. [31] ➢ Shiyu Ji et al. [38] ➢ Amarjit Malhotra et al. [85] ➢ Y.C. Hu et al. [40]
Ripple effect	➢ Continuous trust management process on SUs	
Parasitic	➢ Appropriate local spectrum sensing controller ➢ Eliminating internal hidden parasite nodes	
Homing	➢ Usage of "dummy packets" throughout the network to equalize traffic volume and thus prevent traffic analysis. ➢ Access control	➢ T.Kavitha et al. [83] ➢ Shahriar Mohammadi et al. [80]

	➢ Reduction in sensed data details ➢ Distributed processing ➢ Strong encryption techniques	
Node Replication Attacks	➢ Random Key Distribution – Keys follow a pattern according to the random key distribution scheme. Key will be termed as "cloned" if the key exceeds a threshold. ➢ SET method wherein network is divided into exclusive subsets. ➢ Real time clone detection techniques have been dealt with wherein each sensor considers the neighbourhood information through a superimposed s-disjunct code and computes a fingerprint. ➢ Cluster head selection-based hierarchical distributed Algorithm LNCA using a Bloom filter mechanism including network reactions. ➢ Compressed Sensing-based Clone Identification (CSI) for static WSNs. ➢ Node-to-Network Broadcasting (N2NB) and Deterministic Multicast (DM) protocols. ➢ Distributed witness-based Detection algorithms Randomized Multicast (RM) and Line Selected Multicast (LSM). ➢ Group/Generation based detection algorithms. ➢ RED protocol executed at fixed intervals of time ➢ Cell division-based algorithms Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC). ➢ A polynomial based space-time-related pair-wise key pre-distribution scheme (PSPP-PKPS or just PSPP) for wireless sensor networks. ➢ A real time neighbour-based detection scheme (NBDS). ➢ A node capture detection scheme. ➢ Memory efficient protocols namely memory efficient multicast with Bloom filters (B-MEM), memory efficient multicast with Bloom filters and Cell Forwarding (BC-MEM), memory efficient multicast with cross forwarding (C-MEM), and memory efficient multicast with cross and cell forwarding (CC-MEM). ➢ Active detection protocol. ➢ A novel clone node detection protocol called randomly directed exploration. ➢ Protocols RAndom WaLk (RAWL) and Table-assisted RAndom WaLk (TRAWL). ➢ Mechanisms based on intersecting sets called CINORA-Inset and restricted cell two-phase authentication model called CINORA-Hybrid. ➢ A note-based randomized and distributed protocol called NRDP. ➢ Group deployment knowledge-based schemes based on the assumption that nodes are deployed in groups. ➢ A distributed protocol that does not need any reliable/trusted entities [66]. ➢ A distributed, deterministic approach [67] which includes initialization, witness node discovery phase, and node revocation phase.	➢ R. Brooks et al. [44] ➢ H.Choi et al. [45] ➢ K.Xing et al. [46] ➢ W. Znaidi et al. [47] ➢ C M Yu et al. [48] ➢ B. Parno et al. [49] ➢ C. Bekara et al. [50] ➢ M. Conti et al. [52] ➢ B. Zhu et al. [54] ➢ F. Fei et al. [56] ➢ L. C. Ko et al. [57] ➢ J. W. Ho [58] ➢ M. Zhang et al. [59] ➢ R. Di Pietro et al. [60] ➢ Z. Li et al.[61] ➢ Y. Zeng et al. [62] ➢ S. Gautam Thakur [63] ➢ X. Meng et al. [64] ➢ J. W. Ho et al. [65] ➢ Y. Sei et al. [66] ➢ C. Kim et al. [67]
Selective Forwarding Attack	➢ Introduction of redundancy (probe multiple path routing) in the network ➢ Multi path routing in combination with random selection of paths to destination ➢ Usage of braided paths with no common link and consecutive nodes	➢ Heena Singh et al. [81] ➢ T.Kavitha et al. [83] ➢ Hanen Idoudi et al. [69]
Alteration, Spoofed and Replay of information:	➢ Encryption technique applied to some of the fields of the header message, to avoid communicating some extra bits. ➢ Use of conventional techniques like packet overhead or the digital signatures for broadcasting authenticated messages. ➢ Usage of efficient protocols like TESLA and symmetric key cryptography.	➢ Heena Singh et al. [81] ➢ T.Kavitha et al. [83] ➢ Shio Kumar Singh et al. [86] ➢ Shahriar Mohammadi [80]

	➢ Tiny Sec & SNEP schemes focus on providing message authenticity, integrity and confidentiality, Semantic security, Data authentication, Replay Protection ➢ Central Certificate Authority ➢ Pair-wise authentication	
Misdirection Internet SMURF attack	➢ Victim node will be scheduled to sleep if the node's network link is flooded with irrelevant information, then for sometime the victim node can be scheduled to sleep. ➢ Using hierarchical routing mechanism ➢ Authorization & Monitoring ➢ Central certificate authority ➢ Pair-wise authentication ➢ Network layer authentication ➢ Acknowledgment verification	➢ Heena Singh et al. [81] ➢ T.Kavitha et al. [83] ➢ Shahriar Mohammadi [80]
Acknowledgement Spoofing	➢ Authentication via encryption of all sent packets and also packet headers ➢ Authentication, link layer encryption and global shared key techniques;	➢ Saurabh Singh et al. [68] ➢ S. Datema [87] ➢ Shahriar Mohammadi et al. [80]
Rushing Attack	➢ Detection of secure neighbours by checking the bidirectional link. ➢ Removing delays ➢ Secure Neighbour Detection, Secure Route ➢ Delegation and Randomized Route Request forwarding ➢ Secure Routing Protocol (SRP) and Modified SRP	➢ Heena Singh et al. [81] ➢ Shahriar Mohammadi et al. [80] ➢ P. Papadimitratos et al. [72] ➢ A. Rawat et al. [73]

V. Future Directions & Conclusion

Ensuring secure transmission and exchange of data in a network has never failed to introduce new challenges to network researchers. In spite of the diligent efforts made to avoid security breaches, some research directions still need to be steered. Some of such similar research directions have been discussed by authors of [3].

(i) Utilizing existing security solutions applicable to other types of wireless networks to CRNs also.
(ii) Ensuring cross layer communication and intense interaction between network layers to combat cross layer attacks.
(iii) Introduction of advanced cryptographic algorithms to identify genuine primary and secondary users and filter off the malicious nodes/users.
(iv) Proposal of efficient spectrum sensing techniques.
(v) Game theory being applied to security management along with spectrum and power management.

The paper has aimed to present a briefly surveyed idea regarding various network layer attacks, possible countermeasures and solutions. Future directions aiming at enhanced network security targets have also been extracted from previous work from [3]. However, sharing information between the network, endpoint, and cloud will undoubtedly be the direction of modern security.

References

[1]. A framework of the PHY-layer Approach to Defense Against Security Threats in Cognitive Radio Networks – Hong Wen – IEEE June 2013.

[2]. International Journal of Advent Research in Computer & Electronics, Vol.1, No.2, April 2014 - Survey: Attacks on Cognitive Radio Mesh Networks, T.Pavan Kumar, Dr.K.Rajasekhara Rao & Dr.V.Srikanth.

[3]. A Survey on Security in Cognitive Radio Networks Mahmoud Khasawneh, Anjali Agarwal Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada {m_khasaw, aagarwal}@encs.concordia.ca - 2014 6th International Conference on CSIT, ISBN:987-1-4799-3999-2.

[4]. Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks 2003, 1(2-3):293–315.

[5]. Fabrice Le Fessant, Antonis Papadimitriou, Aline Carneiro Viana, Cigdem Sengul, Esther Palomar. A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis. Computer Communications35, pp. 234-248, 2012.

[6]. Detecting Sinkhole Attack in Wireless Sensor Network Vinay Soni1, Pratik Modi2, Vishvash Chaudhri2 1,2 Department of Computer Engineering, LDRP -ITR, Gujarat Technological University, International Journal of Application or Innovation in Engineering & Management (IJAIEM) Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com Volume 2, Issue 2, February 2013 ISSN 2319 – 4847.

[7]. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011, DOI : 10.5121/ijnsa.2011.3614 185 EFFICIENT DETECTION OF SYBIL ATTACK BASED ON CRYPTOGRAPHY IN VANET Mina Rahbari and Mohammad Ali Jabreil Jamali.

[8]. Classification on Attacks in Wireless Ad Hoc Networks: A Game Theoretic ViewXiaojuan Liao*, Dong Hao*, and Kouichi Sakurai Department of Informatics, Kyushu University Fukuoka, 819-0395, Japan

[9]. Sowmya P, V. Anitha, Defence Mechanism for SYBIL Attacks in MANETS using ABR Protocol, International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-4 Number-2 Issue-15 June-2014.

[10]. Anitha V, Akilandeswari J, Sowmya P, "Auto Defence Mechanism for SYBIL Attacks in Manets using QABR Protocol," 2014

International Conference on Advances in Electronics, Computers and Communications (ICAECC).

[11]. Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen, “SPINS: Security Protocols for Sensor Networks”, Department of Electrical Engineering and Computer Sciences, University of California, Berkley, 2002.

[12]. Effect of Black Hole Attack on MANET Routing Protocols - Jaspal Kumar, M. Kulkarni, Daya Gupta, Panipat Institute of Engineering & Technology, India National Institute of Technology, Karnataka, India Delhi College of Engineering, University of Delhi, India I. J. Computer Network and Information Security, 2013, 5, 64-72.

[13]. A trust based approach for AODV protocol to mitigate black hole attack in MANET Fidel Thachil#, K C Shet# #Department of Computer Science and Engineering, National Institute of Technology, Karnataka - 2012 International Conference on Computing Sciences

[14]. A Trusted AODV Routing Protocol for Mobile Ad Hoc Networks. PhD thesis, Department of Computer Science and Engineering, The Chinese University of Hong Kong, 2003.

[15]. Seungjin Park, M. Al-Shurman and Seong-Moo Yoo. Black Hole Attack in Mobile Ad hoc Network, ACMSE'04, Huntsville, AL, U.S.A., April, 2004.

[16]. Y.C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,” Proc. 8th Ann. Int’l Conf. Mobile Computing and Networking (MobiCom’02), ACM Press, 2002.

[17]. Slavisa Sarafijanovic and Jean-Yvess Le Boudec. An Artificial Immune System Approach With Secondary Response for Misbehaving Detection in Mobile Ad hoc Networks,16, IEEE September 2005.

[18]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[19]. Prevention of Black Hole Attack in MANET Pooja Jaiswal Computer Science & Engineering, Madan Mohan Malviya, Engineering College, Gorakhpur, Uttar Pradesh, India

[20]. E.Padilla, N.Aschenbruck, P.Martini, M.Jahnke and J.Tolle, “Detecting Black Hole Attack in Tactical MANETs using Topology Graph”, Proc. IEEE Conference on Local Computer Networks, 2007.

[21]. M. Medadian, M.H. Yektaie and A.M. Rehmani, “Combat with Black Hole Attack in AODV Routing Protocol in MANETs”, Proc. IEEE Asian Himalayas International Conference on Internet, Nov. 2009.

[22]. X.Y. Zhang, Y. Sekiya and Y. Wakahara, “Proposal of a Method to Detect Black Hole Attack in MANETs”, Proc. IEEE International Symposium on Autonomous Decentralized System ISADS, 2009.

[23]. International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 1, January 2012) - Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method - Disha G. Kariya1, Atul B. Kathole2, Sapna R. Heda3 1Jawaharlal Darda Institute of Engineering & Technology,Yavatmal, India 2Jawaharlal Darda Institute of Engineering & Technology,Yavatmal, India.

[24]. Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks - 1Isaac Woungang, 2Sanjay Kumar Dhurandher, 1Rajender Dheeraj Peddi, and 4Mohammad S. Obaidat, Fellow of IEEE and Fellow of SCS – 2012 IEEE.

[25]. Simulation study of Black hole and Jellyfish attack on MANET using NS3

[26]. Nidhi Purohit, Richa Sinha and Khushbu Maurya - INSTITUTE OF TECHNOLOGY, NIRMA UNIVERSITY, AHMEDABAD – 382 481, 08-10 DECEMBER, 2011.

[27]. G.Xiaopeng and C.Wei, “A Novel Grey Hole Attack Detection Scheme for Mobile Ad-Hoc Networks”, Proc. IFIP International Conference on Network and Parallel Computing, 2007.

[28]. C. Wei, L. Xiang, B. Yuebin and G.Xiopeng, “A New Solution for Resisting Grey Hole Attack in Mobile Ad Hoc Networks”, Proc. IEEE Conference on Communication and Networking, China 2007.

[29]. J.Sen, M.Chandra, S.G. Harihara, H.Reddy and P.Balamuralidhar, “A Mechanism for Detection of Gray Hole Attacks in Mobile Ad Hoc Networks”, Proc. IEEE International Conference on Information Communication and Signal Processing ICICS, Singapore, Dec. 2007.

[30]. International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 1, January 2012) - Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method - Disha G. Kariya1, Atul B. Kathole2, Sapna R. Heda3 1Jawaharlal Darda Institute of Engineering & Technology,Yavatmal, India 2Jawaharlal Darda Institute of Engineering & Technology,Yavatmal, India.

[31]. Improving AODV Protocol against Blackhole Attacks Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri - Proceedings of the International MultiConference of Engineers and Computer Scientists 2010, Vol II.

[32]. A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks Majid Meghdadia, Suat Ozdemirb & Inan Gülerc- IETE Technical Review - Published online: 01 Sep 2014.

[33]. Dhara Buch, Devesh Jinwala. Prevention of wormhole attack in wireless sensor network. International Journal of Network Security & Its Applications (IJNSA), Vol. 3, No. 5, Sep 2011.

[34]. Ritesh Maheshwari, Jie Gao, Samir R Das. Detecting wormhole attacks in wireless networks using connectivity information.

[35]. S. Keer and A. Suryavanshi , To prevent wormhole attacks using wireless protocol in manets, In Int’l Conference on computer science and technolog y |ICCCT’2010|.

[36]. Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung. In 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.

[37]. Mahdi Taheri, Dr.majidnaderi and Mohammad BagherBarekatain. New Approach for Detection and defending the wormhole Attacks in Wireless Ad Hoc Networks. Proceesings of ICEE 2010, May 11-13, 2010.

[38]. Gunhee Lee, Dong-kyoo Kim, JungtaekSeo. An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks. International Conference on Information Security and Assurance, 2008.

[39]. Wormhole Attack Detection Algorithms in Wireless Network Coding Systems Shiyu Ji, Tingting Chen, and Sheng Zhong - IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 3, MARCH 2015

[40]. A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks Majid Meghdadia, Suat Ozdemirb & Inan Gülerc- IETE Technical Review - Published online: 01 Sep 2014.

[41]. Y.C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. IEEE INFOCOM, Mar 2003.

[42]. RiteshMaheshwari, JieGao, Samir R Das. Detecting Wormhole Attacks in Wireless Networks. In IEEE, 2006 pages 109-111, IEEE INFOCOM 2007

[43]. Cognitive radionetworksecurity:Asurvey Sazia Parvin a, FarookhKhadeerHussain b,n, OmarKhadeerHussain a, SongHan a, BimingTian a, Elizabeth Chang

[44]. Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey - Wazir Zada Khan,1 Mohammed Y. Aalsalem, Mohammed Naufal Bin Mohammed Saad,1 and Yang Xiang - International Journal of Distributed Sensor Networks Volume 2013, Article ID 149023.

[45]. R. Brooks, P. Y. Govindaraju,M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Transactions on Systems, Man and Cybernetics C, vol. 37, no. 6, pp. 1246–1258, 2007.

[46]. H. Choi, S. Zhu, and T. F. L. Porta, "SET: detecting node clones in sensor networks," in Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm '07), pp. 341–350, September 2007.

[47]. K.Xing, X. Cheng, F. Liu, andD.H.C.Du, "Real-time detection of clone attacks in wireless sensor networks," in Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS '08), pp. 3–10, Beijing, China, July 2008.

[48]. W. Znaidi, M. Minier, and S. Ubeda, "Hierarchical node replication attacks detection in wireless sensors networks," in Proceedings of the 20th IEEE Personal, Indoor and Mobile Radio Communications Symposium (PIMRC '09), pp. 82–86, Tokyo, Japan, September 2009.

[49]. C. M. Yu, C. S. Lu, and S. Y. Kuo, "CSI: compressed sensing based clone identification in sensor networks," in Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops '12), pp.290–295, Lugano, Switzerland, March 2012.

[50]. B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proceedings of the IEEE Symposiumon Security and Privacy (IEEE S and P '05), pp. 49–63, May 2005.

[51]. C. Bekara and M. Laurent-Maknavicius, "A new protocol for securing wireless sensor networks against nodes replication attacks," in Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications(WiMob '07),White Plains, NY, USA, October 2007.

[52]. C. Bekara and M. Laurent-Maknavicius, "Defending against nodes replication attacks on wireless sensor networks," 2012, http://www-public.it-sudparis.eu/ lauren m/articles/bekara- SARSSI07.pdf.

[53]. M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '07), pp. 80–89, September 2007.

[54]. detection of clone attacks in wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685–698, 2011.

[55]. B. Zhu,V. G. K.Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC '07), pp. 257–266, Miami

[56]. Beach, Fla, USA, December 2007.

[57]. B. Zhu, S. Setia, S. Jajodia, S. Roy, and L.Wang, "Localizedmulticast: efficient and distributed replica detection in large-scale sensor networks," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 913–926, 2010.

[58]. F. Fei, L. Jing, and Y. Xianglan, "Space-time related pairwise key predistribution scheme for wireless seneor networks," in Proceedings of the International Conference onWireless Communications, Networking andMobile Computing (WiCOM '07), pp.

[59]. 2692–2696, Shanghai, China, September 2007

[60]. L. C. Ko,H. Y. Chen, and G. R. Lin, "Aneighbor-based detection scheme for wireless sensor networks against node replication attacks," in Proceedings of the International Conference on Ultra Modern Telecommunications and Workshops (ICUMT '09), pp.

[61]. 1–6, St. Petersburg, Russia, October 2009.

[62]. J. W. Ho, "Distributed detection of node capture attacks in wireless sensor networks," in Smart Wireless Sensor Networks, H.D. Chunch and Y. K. Tan, Eds., pp. 345–360, InTech, Rijeka, Croatia, 2010.

[63]. M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in Proceedings of the 17th IEEE International Conference on Network Protocols (ICNP '09), pp. 284–293, Princeton, NJ, USA, October 2009.

[64]. R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Data security in unattended wireless sensor networks," IEEE Transactions on Computers, vol. 58, no. 11, pp. 1500–1511, 2009.

[65]. Z. Li and G. Gong, "Randomly directed exploration: an efficient node clone detection protocol in wireless sensor networks," in Proceedings of the 6th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS '09), pp. 1030–1035, Macau,

[66]. China, October 2009.

[67]. Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random walk based approach to detect clone attacks in wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol. 28, no. 5, pp. 677–691, 2010.

[68]. S. Gautam Thakur, "CINORA: cell based identification of node replication attack in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications Systems (ICCS '08), 2008.

[69]. X. Meng, K. Lin, and K. Li, "Note based randomized and distributed protocol for detecting node replication attack," in Algorithms and Architectures for Parallel Processing, vol. 6081 of Lecture Notes in Computer Science, pp. 559–570, 2010.

[70]. J.W.Ho, D. Liu, M. Wright, and S. K. Das, "Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1476–1488, 2009

[71]. Y. Sei and S. Honiden, "Distributed detection of node replication attacks resilient to many compromised nodes in wireless sensor networks," in Proceedings of the 4th Annual International Conference onWireless Internet (WICON '08), 2008.

[72]. C. Kim, S. Shin, C. Park, and H. Yoon, "A resilient and efficient replication attack detection scheme for wireless sensor networks," IEICE Transactions on Information and Systems, vol. 92, no. 7, pp. 1479–1483, 2009.

[73]. Security For Wireless Sensor Network Saurabh Singh Department of Computer Science and Engineering, NIT Jalandhar Punjab, India Dr. Harsh Kumar Verma Department of Computer Science and Engineering, NIT Jalandhar Punjab, India - Saurabh Singh et al. / International Journal on Computer Science and Engineering (IJCSE)

[74]. Security Challenges in Cognitive RadioNetworks Hanen Idoudi, Kevin Daimi, and Mustafa Saed, Proceedings of the World Congress on Engineering 2014 Vol I, WCE 2014, July 2 - 4, 2014, London, U.K.

[75]. Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim Networks and Systems Laboratory University of Badji Mokhtar Annaba, Algeria - 2013 UKSim 15th International Conference on Computer Modelling and Simulation

[76]. J.V. Mulert, I. Welch and K. G. W. Seah, "Review: Security threats and solutions in MANETs: A case study using AODV and SAODV," Journal of Network and Computer Applications, vol. 35, issue 4, Jul. 2012, pp. 1249-1259,doi:10.1016/j.jnca.2012.01.019.

[77]. P. Papadimitratos, Z.J. Haas and P. Samar, "The Secure Routing Protocol (SRP) for Ad Hoc Networks", IETF Internet Draft , December 2002, available at http://www.ietf.org/proceedings/56/I-D/draftpapadimitratos- secure-routing-protocol-00.txt.

[78]. A. Rawat, P.D. Vyavahare and A.K. Ramani, "Evaluation of Rushing Attack on Secure Message Transmission (SMT/SRP) Protocol

for Mobile Ad Hoc Networks", Proc. International Conference on Personal Wireless Communications (ICPWC), Jan. 2005.

[79]. L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 492–503, 2009.

[80]. M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in Proceedings of the International Symposium on aWorld ofWireless,Mobile and Multimedia Networks (WoWMoM'06), pp. 564–568, June 2006.

[81]. K. SSu, W. Wang, and W. Chang, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," Computer Networks, vol. 53, no. 18, pp. 3042–3056, 2009.

[82]. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER 2013 A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks Adnan Nadeem, Member, IEEE, and Michael P. Howarth

[83]. Security Threats in Mobile Ad Hoc Network - Kamanshis Biswas and Md. Liakat Ali, Master Thesis - 2007, Department of Interaction and System Design School of Engineering Blekinge Institute of Technology, Sweden.

[84]. Network Layer Attacks and Defense Mechanisms in MANETS- A Survey, International Journal of Computer Applications (0975 – 8887) Volume 9– No.9, November 2010, G.S. Mamatha Assistant Professor, ISE Dept. R.V. College of Engineering Bangalore, Dr. S.C. Sharma Vice Chancellor Tumkur University Tumkur, Karnataka.

[85]. A Comparison of Routing Attacks on Wireless Sensor Networks Shahriar Mohammadi1; Reza Ebrahimi Atani2, 3 and Hossein Jadidoleslamy - Journal of Information Assurance and Security ISSN 1554-1010 Volume 6 (2011) pp. 195-215.

[86]. A Study on Security Threats and Their Countermeasures in Sensor Network Routing - International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014 - Heena Singh1, Monika Agrawal2, Nidhi Gour3, Prof. Dr. Naveen Hemrajani4 - International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014.

[87]. Sanket S. Kalamkar, Adrish Banerjee, Ananya Roychowdhury, Malicious user suppression for cooperative spectrum sensing in cognitive radio networks using Dixon's outlier detection method, in: 2012 National Conference on Communications (NCC), 2012, pp.1–5 (IEEE).

[88]. Security Vulnerabilities In Wireless Sensor Networks: A Survey - T.Kavitha, D.Sridharan, Anna University, Journal of Information Assurance and Security 5 (2010) 031-044

[89]. Virendra Pal Singh, Sweta Jain, Jyoti Singhai. Hello flood attack and its countermeasures in wireless sensor networks. IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.

[90]. Wormhole Attack Prevention using Clustering and Digital Signatures in Reactive Routing Amarjit Malhotra, Deepti Bhardwaj, Ankush Garg, Division of Information Technology, Netaji Subhas Institute of Technology, University of Delhi, New Delhi, In

[91]. International Journal of Computer Trends and Technology- May to June Issue 2011 ISSN: 2231-2803 1 IJCTT A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks Shio Kumar Singh 1, M P Singh 2, and D K Singh 3

[92]. S. Datema. A Case Study of Wireless Sensor Network Attacks. Master's thesis, Delft University of Technology, September 2005.