CHAPTER 4

ADVANCED SECURED MODEL FOR ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL IN MANET

4.1 INTRODUCTION

In recent times, the Mobile Ad-hoc networks (MANET) are finding its use in many applications. MANET is a temporary network formed by a collection of mobile nodes that operates without depending on centralized administration or usually available standard support devices as that of other conventional networks. As the nodes usually have a limited transmission range, every node requires the assistance from its neighboring nodes in forwarding packets. The nodes act both as routers and hosts in an ad-hoc network and hence the task of forwarding packets between nodes and running user applications can be carried out by a node. In case of situations having no fixed infrastructure and deploying network, Ad-hoc networks play a significant role. This means the application of ad-hoc mobile networks in several important fields such as military, emergency, conferencing and sensor networks each of which have specific requirements for routing protocols.

The MANET structure is more exposed to attack when compared to the wired network and the vulnerabilities are difficult to remove due to the nature of MANET. This drives the need for exploiting the vulnerability of attacks having malicious features so as to cripple the MANET operation. The immediate security measures to reduce the event of attacks include prevention measures such as authentication and encryption. However, limitation exists in such techniques due to its design for only known set of attacks thus lacking the complete prevention. The newer attacks tend to bypass the existing prevention
measures thus requiring potential security techniques. This shows the need for operating a robust MANET with higher security.

In the present research, the advanced secured model for On-demand Distance Vector (AODV) routing protocol is proposed to ensure security. The proposed protocol offers high security against Denial of Service (DoS) attack and Black Hole (BH) attack. Better performance in terms of packet delivery ratio, normalized routing load and the average throughput are also the advantages of this protocol.

4.1.1 Denial of Service (DoS) Attack

MANETs with its salient features become vulnerable to Denial of Service (DoS). Hence, a cooperation based incentive mechanism is necessary among nodes in the network to improve the performance of overall network by reducing DoS attacks. In the work of Denko and Mieso (2005), a reputation-based incentive mechanism has been proposed to detect as well as prevent DoS attacks. The investigation of DoS attacks caused by selfish and malicious nodes has been performed. In present research, the proposed method encourages cooperation of nodes failing on which it is being excluded from the network. The performance of the present method is evaluated by means of packet delivery ratio, the routing and communication overhead, and misbehaving node detection in a discrete event-simulation environment. The results have shown the significant reduction of DoS attacks and simultaneous improvement in MANETs performance on employing reputation-based incentive mechanism.

Wood & Stankovic (2002) have worked on the problem of reduction in the performance of expected function of a network’s capacity due to diminishing or elimination of an event. By launching such attacking events against server resources or network bandwidth, authorized users are prevented from accessing resources for instance, in websites having larger access such as
Amazon, eBay and so on. The consequence of such attacks ranges from temporary blocking of available service to permanent distortion of network information. The target of DoS attacks can be either a client computer or a server computer. For example, a system gets targeted by the attack in terms of exhaustion of limited wireless resources such as bandwidth, storage space, battery power, CPU, or system memory. However, data integrity of networks and applications get targeted directly by modifying routing information or system configuration.

In MANETs, nodes take the role of both routers and ordinary nodes. The underlying new challenge in networking communities is the network security which has arisen as the result of dynamic network topology and lack of centralized infrastructure. Compared to other traditional networks, MANETs are more prone to DoS attacks owing to the limited resources available in forcing the nodes for resource utilization. The lack of cooperation even among the activities of smaller set of nodes would significantly result in decreased network performance. This can be explained by an example of network congestions caused due to repeated retransmissions by a misbehaving node while discarding any packets that passes through it. Unlike wired links, the wireless link does not offer the protection for data transmissions. This leads to the interference by any user or receiver with data packets or routing information. Another critical means that require attention is the battery power of mobile nodes. If some malicious attacks like sleep deprivation attack drains up the battery power, the network services get stopped. The mobility of the nodes, changes in network connectivity and available resource also results in exposure of a network to various attacks.
DOS attack scenario

There are three broad groups that categorize the type of DoS attacks that target resources. The first group of attack aims on Storage and Processing Resources. The memory, storage space or CPU of the service provider is mainly targeted by this attack. If in case of an executable flooding packet is sent continuously by a node, the storage space is overloaded which deplete the node’s memory. The node is also prevented from sending or receiving packets from other legitimate nodes. The prevention of such events takes place by means of monitoring to gradually exclude such malicious nodes. The energy resources, in particular the battery power of the service provider gets attacked by the second group of attack. Energy becomes an important resource in MANETs as the mobile devices are operated by battery power. The battery energy of the victim gets continuously consumed by a malicious node. It is done by sending a bogus packet to a node and also by preventing other nodes from communicating with the node. The detection of such malicious nodes is possible using localized monitoring to prevent the consequences.

The third means of attack aims on bandwidth. For example, in the case of locating the attacker between multiple communicating nodes, the network bandwidth gets destroyed to disrupt connectivity. The network overloading takes place when bogus is continuously sent by the malicious nodes with source IP addresses of other nodes. This results in the consumption of neighbor’s resources that involved in communication and network overloading thus leading to performance degradations. The prevention of such attacks can be possible using exchange of repudiated information among the involved nodes or the cluster head.
Defending Against DoS Attacks

In order to handle DoS attacks, two main schemes such as detection and prevention are used. The detection helps to locate an attacker for taking necessary actions. The source of attacking DoS can be detected by monitoring the activity of nodes to trace an attacker. In the work of Habib et al. (2003), several tracing and monitoring mechanisms are proposed which involve core-based and edge-based monitoring, deterministic and probabilistic packet marking. Before launching the prevention mechanism, it helps to thwart DoS attacks. The attack packet is identified to take preventive action before it reaches the intended target. The method of ingress or egress filtering and route-based packet-filtering mechanisms is commonly used for the internet.

(Source: Habib et al. 2003)

Figure 4.1 Distributed Denial of Service Attack
The denial of service attack can be prevented by launching the control either from a single host or from multiple hosts. Distributed Denial of Service (DDoS) attacks are originated from distributed multiple hosts in the network whereas single-source denial of service (SDoS) attacks are generated from a single host. However, some literature implies DoS as the single-source denial of service. So to avoid the contrary, DoS in this work is referred as both distributed and single source attacks and clearly stated if it is distributed or single source when clarification is required.

There are two typical types of DDoS attack components such as agents and a handler. The agents run on compromised hosts for generating the actual attack messages whereas the handler controls the agent by giving instruction on the method and timing of attack (Scarfone et al., 2008). Agents are also called as bots which are run by a collection of hosts and botner is a single attacker that controls the bots. The steps for executing a typical DDoS attack are illustrated in the Figure 4.1. The first step is to compromise the vulnerable hosts in the Internet and to deploy the attack tools (agents) on the hosts. Second step is the dissemination of an attack command from the handlers to the agents which instructs the agents about the method of attacking. The generation of traffic by the agents starts at the instructed attack time towards the target to perform the attack. Another class of DDoS attacks involve in exploitation of vulnerabilities rather than the exploited hosts to generate the attack traffic. In such types of attack, the exploited hosts are called as unwitting agents.

**Targets of DoS**

The end victim targeted by a DoS attack will be anyone among computer that implements all layers of OSI reference model (Shirey, 2007), a router, ongoing communication, a link or an entire network, an infrastructure, or any combination of or any variant of these(Handley et al., 2006). The
targeted victim can however an application, or an operating system in case of an end system. Here, the term end system denotes either an “Internet host” or “end host” or sometimes “host”. The end host or host represents the computer that implements all five layers of TCP/IP protocol stack (Braden, 1989).

**DoS on application**

In case of DoS attacks on an application, an attacker helps in preventing the application from carrying out its intended tasks by exhausting the finite supply of a specific resource (Chang et al., 2002).

**DoS on operating system**

The DoS attacks on operating system works in the same manner as DoS attacks on application. However, the problem of protecting the operating system becomes more sever in case of DoS attacks on operating system.

**DoS on router**

The DoS attacks that are launched against an end system can be similar as to that of an IP router. Routing protocols can also be used in addition to start a DoS attack on a router or a network of routers. The generation of the relevant routing messages has probably leads to the ability of sending traffic. The routing table is overload by the simplest attack on a router when either a sufficiently large number of routes go out of the memory or when the router has inadequate CPU power to process the routes (Nordstrom and Dovrolis, 2004). The use of false route updates tends to cause more serious DoS attacks on routers by causing black hole in an entire network address block (Xing et al. 2006).
DoS on ongoing communication

Rather than attacking the end system, an attacker tends to disrupt an ongoing communication. While observing a TCP connection, the task of spoofing packets takes place easily to either reset or to de-synchronize the connection to ensure no further progress. When an attacker could not observe a TCP connection, but finds the connection, it is again possible to reset or de-synchronize that connection. It is possible by sending large number of spoofed TCP reset packets which presumes the TCP port number and TCP sequence number.

DoS on links

The DoS attack on links can be simply defined by sending enough non-congestion-controlled traffic (e.g., UDP traffic) so as to excessively congest and hence legitimate traffic faces the problem of excessively high packet loss. In case of losing sufficient routing packets, an adjacency could be dropped and the effects of the attack get potentially amplified by congesting a link using routing protocol. Further, an attacker sometimes refuses an access to a link. This is attributed to the router for generating sufficient monitoring or reporting traffic so that to fill the link.

Security aspect

In Mobile Ad-hoc Networks, the DoS attack is considered as one of the most serious attacks and hence efficient protocols to defend such attack requires the ability to encounter the issues of node movement, lacking wireless connection and scalability. Further, launching an appropriate attack on the entire available resources of the network is possible by attacking one single physical device in the mobile ad-hoc network. While sending voluminous segments to the victim machine, the attack become serious due to the
simultaneous cooperation of distributed large number of nodes through the network.

In MANETs, DoS attacks consume bandwidth, battery energy or CPU cycles that are considered as scarce system resources and also separate legitimate users from a network. Hence the impact of DoS attacks threatens the network connectivity and also undermines the control and data message delivery functions of the network. The deep insight into DoS attacks and their impacts on MANETs have been presented in the study by Paxson (1998). The node isolation problem due to DoS attacks has been analyzed initially for deriving the probability of node isolation. This further leads to exploitation of fraudulent routing messages such as Black Hole attack that affects the connectivity more severely compared to others. Secondly, a dynamic DoS attack has been introduced as the node mobility and potential attack propagation have not been considered previously in the study of DoS attack. The dynamic DoS attack tends to progress the new DoS attacks as it characterized by exploiting the node mobility, dynamic power control, and compromised nodes. An analytical study on the features of new DoS attack such as its potential devastating impact on the MANETs connectivity has been explained.

**Dynamic Dos Attacks and Impacts**

Some DoS attacks such as Black Hole or Jellyfish are called as static DoS attacks understood as the node mobility or potential attack propagation have not been considered. The method of dynamic adjustment of transmission power and propagation of DoS attacks takes place when the malicious nodes move around the entire network by compromising their cooperative neighbors. Hence, dynamic operation of the DoS attacks in terms of the expansion of attack coverage and the propagation of attack impact will be resulted. This
section introduces dynamic DoS attacks and exposes its devastating impact on MANETs by giving several examples.

**Dynamic DoS Attacks – A Scenario Overview**

**Dynamic DoS Attack Using Node Mobility**

As the malicious nodes are mobile, there exists spreading of the impact of DoS attacks. This is illustrated in Fig. 4.2 (left), as a malicious node m first attacks its three neighbor’s v1, v2 and v3. Once the communications among its neighbors and other cooperative nodes are prevented by node m, it continues to launch DoS attacks against other new neighbors by moving to another place as shown in Figure 4.2 (right). If the malicious node u moves into an area with a higher node density, then more cooperative nodes may become the victims of DoS attacks.

(Source: Molsa 2005)

**Figure 4.2 DoS attack enhanced by malicious nodes movement**

**Dynamic DoS Attack Using Power Management**

In case of dynamic adjustment of their transmission power by the malicious nodes, then transmission ranges can be changed for spreading the attack coverage. As shown in Figure 4.3, when a source node s requires communication with a destination node d, node s requests for route discovery
its neighbors. If the forwarded request message is received by the malicious node m, its transmission power gets immediately increased by means of increasing transmission range from R to $R'$ in order to reach node s in one hop. Then, node m can unicast a route reply message to node s for claiming only one hop away from the destination d. This mechanism is an alternate to Black Hole attack however being aggressive it disturbs the cooperative nodes beyond one-hop neighborhood.

(Source: Molsa 2005)

Figure 4.3 DoS attack enhanced by dynamic power control

The effect of DoS attacks becomes serious on the computing systems as it attempts to prevent the machine or network Resources unavailable to its intended users. The victim which could be a host, a router, or an entire network becomes severely degraded by the DoS attacks. The continuous increase in number of DoS attacks seriously threatens the availability of network services. This necessitates the effective mechanisms for detecting DoS attacks.
Denial of service attack usually blocks a node from receiving legitimate data or completely from another legitimate node. This method of blocking is either done by sending continuous data or radio signals. The victims of Dos attach include Software System, Network Router, Server and End-User PCs. The attack operates by denying or degrading normal services for legitimate users. This is done by sending huge traffic to the victim (machines or networks) so that the services get exhausted thus losing connection capacity or the bandwidth. The severe degradation of the efficiency of the online services results due to denial of service attack. Hence, it must be effectively detected for protecting the online services. The main role of the DoS attack detection is to develop network-based detection mechanism by mean of two types of detection system such as misuse detection (Garcia-Teodoro et al., 2009), and anomaly detection (Karjee & Banerjee).

There exist two basic forms for launching DoS attacks such as software exploit and flooding. In the software exploits attack, the attacker node involves in sending few packets to use specific software bugs within the target node application. This attack can be prevented by addressing adequate software fixes.

Service (DoS) attacks and grey hole attack has been explained in the work of Jin-Hee Cho et al. (2011). The neighboring nodes trust scores has been introduced and avoids the misbehaving neighbor nodes in the route discovery process. Hence, the trust based routing protocol improves the data integrity at receiver node (Abdelaziz et al. 2013, Jie et al. (2008) and Hejmo et al. (2006)). The current research field aims to develop stable and secure design of routing protocols in MANET as it the attacks are considered as the most disturbing problem in MANET. Especially in applications like military service, successful DoS attacks will lead to several dangerous consequences (Jhaveri et al. (2012), Khurana et al. (2006)). The malicious node either disables or
increases the DoS attacks as Route request rate limit gets overridden for putting up the restriction. The parameter called RREQ_RATELIMIT is set for selecting a very high value by the adversary node thus leading to the flooding of fake RREQ network causing DoS attack. As the network load is forced by false RREQ packets, the node in the DoS attack faces difficulty in serving other nodes. This attack finally results in affecting the entire discovery process of the network. In this research, effective detection of DoS attacks is done by secured AODV protocol DoS attacks.

4.1.2 Security Concerns

The extensive usage and application of MANET depends on the security component. The unique characteristics of MANETs include both continuous and dynamic changing network. The problem faced by the conventional networks to directly use the existing security system is due to the resource constraints such as bandwidth and the limited battery power (Chien-Chung et al. 2003). The active or passive violation of the entire goals of security like availability, integrity, confidentiality, access control, non-reputation and authentication leads results in MANETs attack (Payal et al. 2009). In this present research, Denial of service (DoS) and Black hole (BH) attacks are focused.

4.1.3 Black Hole Attack

The malicious node initiates route request packet in black hole (BH) by hanging around the attack for neighbor node. False RREQ having altered high series number have been sent once after receiving the RREQ packets. Thus the source node thinks about the nodes with new routes towards the destination. The source node also ignores the received RREP packet from other nodes for sending the packets over the malicious node. The complete route has been thus required by the malicious node. Thus the data packets are ingested by
ignoring it to forward elsewhere (Dokurer & Semih (2006), Alem et al. (2010), Perkins et al. (2003)).

4.2 METHODOLOGY FOR SECURE MODEL

The present work describes the proposed method in terms of framework, architecture, maintenance, route discovery and attack prevention. There are two main phases in the proposed protocol such as route maintenance and route discovery phase. The design includes three modules such as direct observation, promiscuous observation, establishment of advanced secured route discovery, route maintenance and attack protection. The means of protecting malicious attacks like DoS and the Black hole attack are focused by the proposed method. The neighbors trust value has been calculated to ensure protection of the proposed design. By introducing the Packet Buffer (PB) and Node Trust Table, the modified AODV routing protocol is proposed for designing a secured model. The information regarding malicious node and neighbor node is saved in NTT. Each node stored the neighbor node ID to calculate the node trust value using the packet observation as shown in expression 4.1.

\[ N_{t_x} = \text{MAX} (0, \text{MIN} (1, (K \cdot T_{XY}) + (1+K) \cdot (T_{XY} + R_c))) \]  (4.1)

In the above equation, K represent constant (K=0.93) and R_c may represent any constants such as RREQ constant, RREP constant, Data constant and Black hole constant. When RREQ constant and RREP constant become equal to 0.3, it represents success whereas it represents failure when constants equal to -0.3. Similarly in case of Data constant, if it is equal to 0.4, it is success and if it is less than -0.4, it is failure. Initially node x trust for y at i_th event (T_{XY}) is equal to 0.5 by default and gets updated on failed and successful transmission.
Black hole constant is set to -7.2 and its minimum trust value and maximum trust value is set as 0 and 1 respectively. The value of threshold is set as 0.5 and packets will be dropped when nodes have the trust value of less than 0.5.

The 3 types of Packet buffer (PB) include PB_DATA, PB_RREQ and PB_RREP. The data packets which is either sent by the node or forwarded from other received nodes are stored and controlled by the Packet Buffer was used to store data packets and control packets depending on Packet Buffer timer and promiscuous mode. This happens while sending and forwarding of RREQ, RREP and DATA of each node to next node.

The functions such as delete, insert, update, search, print table and access entries of Node Trust Table are performed by the Packet Buffer for updating observation based neighbors trust value. The deletion of the expired from the buffer occurs at the predefined interval.

4.2.1 System Model

Considering the Mobile ad-hoc network model with a set of nodes given by: \( N = \{N_1, \ldots, N_n\} \), where \(|N| = n\), the MANET network avoids the centralized source as like wireless MANET networks (Jin et al.. 2004). The \( n \) nodes of the MANET consist of MANETs having added capabilities along with administrative and control tasks of the network (cluster heads and data aggregation points. The definition of victim nodes in the works of Zhang et al.. (2010) is represented as a set of nodes \( T = \{T_0, \ldots, T_{r-1}\} \), where \( T \subseteq N \), such that, each target node \( r \) of set \( T \) is a critical node of the network, and \(|T| = r \ll n\). The adversary-class is defined as the set of malicious nodes in the network, and are denoted as: \( A = \{A_0, A_1, \ldots, A_{k-1}\} \), where \(|A| = k \leq n\).
In case of communication based on MANET, random topology helps to forward the traffic packets originating from a source node by the nodes through a set of intermediary nodes. In this approach, AODV model is proposed however with improved protection. The protection is ensured by calculating the neighbors trust value and Node Trust Table. The modification of AODV routing protocol helps in designing an advanced security model called Enhanced AODV (EAODV). In this process, Enhanced AODV protocol is used as the employed distributed model is similar to the one presented by Chuiyi et al. (2011). The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad-hoc network. The protocol enables to quickly adapt itself for dynamic link conditions, low processing and memory overhead, low network utilization so as to determine the destination of the unicast routes within the ad-hoc network. The destination sequence numbers are used to ensure loop freedom at all even at the time of facing an anomalous delivery of routing control messages to avoid problems such as "counting to infinity" linked with classical distance vector protocols.

4.2.2 AODV Overview

In the work of Abusalah et al. (2008), the most popular reactive routing protocol, AODV consisting of phases such as route maintenance, route discovery and neighbor maintenance have been researched dynamically. While sending the data packets from source node S to a destination node D, the route discovery phase gets initiated by broadcasting RREQ packets to its neighbor nodes.

The received RREQ packets will be rebroadcasted to their own neighbors and the broadcast continues until the RREQ packets reach the destination node D. Before receiving RREQ message, the RREP message gets back from node D to node S. The same route that receives the route request messages replies the message back to the same route. The delayed RREQ
messages will be ignored and the date transmitted through this route is considered as discovered path. Further, AODV enables the intermediate nodes which have adequate fresh routes for sending and generating RREP to source node.

4.2.3 Threshold based EAODV (T-EAODV) for DDOS attack detection

In the process of DDOS attack, a large set of hoax packets has been generated by the malicious nodes for enabling transfer towards a group of selected target nodes present at critical network locations. On the whole, the existing network includes the attacker nodes as it implies compromised but legitimate MANET nodes (Kong et al. 2003). Moreover, the adversary class injects the nodes into the network in order to make them participate in the attack traffic generation process. On successful completion of attack, the legitimate nodes of the network are replaced by the injected nodes to generate false (misleading) data for destination transfer and delivery. The single detector node observes the attack launched from a single entry point of the network. In contrary, a distributed denial of service attack has been described by Ahamad et al. (2015). The protocol needs a coordinated effort using a set of detector nodes that are present at various MANET locations for accurate detection of such attacks. Similar to the work presented by Timcenko et al. (2012), the present attack detection scheme performs detection of such attacks while launched by both injected MANET and laptop-class nodes.
As shown in Figure 4.4, G is considered as the set of detector nodes (Graph Neurons (GN)) with n number of nodes in the network. The selected decision making nodes in MANET is the Master GN (mGN) as proposed by Patil et al. (2016). The attack detector nodes promiscuously generated and transited monitor traffic packets by means of respective local neighborhoods.

Similar to the work of Xiang et al. (2011), the nodes are also programmed to coordinate and exchange traffic observation messages with
neighboring (peer) GN nodes to perform pattern reconstruction and traffic observation verification. For example, the traffic observation sub-patterns are exchanged between GN node GN$_i$ with its respective GN nodes GN$_{i-1}$ and GN$_{i+1}$. This exchange process is performed by each GN node, at an interval of time equals to $\Delta_{opt}$. The reason for exchanging the traffic sub-pattern values includes a) verification of the observed readings with peer GN nodes, and b) reconstruction of partial patterns of observed traffic, from peer traffic observation readings. Upon reconstruction, the complete observed traffic pattern for a given target node $r$ is defined as the concatenation of all observed sub-pattern values, $p_1^r, p_2^r, ..., p_n^r$ observed by the GN nodes. For instance, sub-pattern $p_n^r$ defines the total observed traffic packets by GN node $n$, destined for target node $r$, within the current time epoch.

As proposed in the work of Abdollah et al. (2010), the maximum packets obtained by a victim node $r$ from the region of operation of GN node $n$ has been depicted by the threshold sub-patterns stored within the threshold table of each GN node. So, $r$ threshold sub-pattern values are exactly hold by each GN node at any given time, one for each of the $r$ target nodes. The total number of traffic packets observed by a GN node denotes the value of the traffic observation sub-pattern which is destined for a given target node at the current time period. To get localized confirmation of anomalous traffic intensities, each GN node compares the observed sub-pattern values with corresponding sub-pattern values in the threshold table. While the actual network time is progressing, the target nodes holds the receding energy content values due to MANET $y$ operations associated with processing both normal as well as malicious packets. Considering this recession in the total energy content values of the target nodes, the total number of message packets receivable by these nodes in the same time interval length $\Delta_{opt}$, must decrease, to ascertain that the node survives its expected lifetime. As a result, the threshold sub-
pattern values for each of the r target nodes, stored in the threshold tables of the GN nodes requires regular updating to reflect these reducing numbers of requests received by the target nodes. After exchanging and reconstructing the sub-patterns for each of the r target nodes of the network successfully, half of the total number of GN nodes of the GN array communicates exactly with their respective designated master nodes named as mGN nodes. The reason for having only half of all the GN nodes communicating with the respective mGN nodes lies on factors such as a) avoiding duplication in the messages received by the mGN nodes and b) reducing the overall communication overhead associated with more number of message transmissions.

Using the Optimal Greedy Algorithm, the source selects the mGN nodes which are a subset of the GN node set during network initialization time. The GN nodes help to collect individual traffic observation messages from the GN nodes for generating a verdict signal to confirm an attack in progress against any or all of the r target nodes. The overall communication overhead associated with the frequent and direct transfer of observation messages from the GN nodes to the source has been reduced owing to the proximity of the mGN nodes to the GN nodes. The number of mGN nodes m is much less than the total number of GN nodes in the network, n. The large number of mGN nodes in the network enables increasing of the overhead on each individual node. This is attributed to the additional tasks of data collection and forwarding performed by the mGN nodes. The presence of few mGN nodes for the detection scheme will increase the overhead on the smaller set of mGN nodes. The overall number of nodes for performing additional mGN-related tasks is consequently reduced. The set of mGN nodes is a subset of GN nodes, with guaranteed reach ability between each mGN node and the set of GN nodes in its respective jurisdiction. The mGN nodes receive reconstructed sub-patterns from their designated GN nodes for generating a delivery message to the source thus depicting either an attack against a target node or a normalcy signal.
indicating smooth network traffic flow at every period of time as described in the work of Choi et al. (2014).

The five phases of operations of DDOS detection process are

- Selection of Decision making nodes & pattern learning
- Node behavior Monitoring
- Communication phase
- Decision making phase
- Pattern Variation Recording

**Selection of Decision making nodes & pattern learning**

The source performs the completion of the initialization phase of the detection scheme at the end of the actual initialization of the MANET network. At this phase, node identification tags and topologies are established in which the scheme initialization step consists of the following two sub-phases:

- Selection of mGN node using Optimal Greedy Algorithm

The GN as well as the mGN nodes is chosen to operate as part of the attack detection process. This is meant for operating such nodes with enough signal observation strength to span their respective regions of operation. The optimal decision making graph neurons called as master GN (mGN) is identified by an efficient Optimal Greedy Algorithm is employed as a heuristic approach as stated. The mGN nodes helps in collecting individual traffic observation messages from the GN nodes to generate verdict signal and to confirm an attack in progress against any or all of the target nodes.
The Optimal Greedy Algorithm starts with the set of selected GNs by having R as the empty set. A new vertex v is added to R in every step whereas v is chosen in a simple and sensible way thus making ratio of the gain in persistence of adding v to R to the selection cost c(v) becomes maximum. The algorithm stops when the persistence \( \pi(G) \) of the network with set of sinks R is at least the required persistence \( \pi_0 \). The algorithm is described by denoting \( \pi(G, R) \) as the persistence of the network G with R as its set of GN nodes. The greedy algorithm for selecting mGN with required persistence is given as follows:

Step 1: initialize \( R := \emptyset \)

Step 2: let \( v \in V(G) \backslash R \) be the vertex for which the maximum

\[
\max_{v \in V(G)} \frac{\pi(G, R \cup \{v\}) - \pi(G, R)}{c(v)}
\]

is attained and let \( R := R \cup \{v\} \)

Step 3: If \( \pi(G, R) \geq \pi_0 \) then return R; otherwise go to step 2.

The Optimal Greedy Algorithm works in polynomial time as the most \( |V(G)| \) iterations are run and each iteration requires at most \( |V(G)| \) persistence computations. Thus the optimal mGN having high probability is chosen for the monitoring purpose. The corresponding values for a given target r in the threshold tables are compared at the end of each time epoch \( \Delta_i \) for deciding the generated output signal sign r \( (\hat{\Delta}_i) \) by each GN node n while transmitting to its designated mGN node, qn. Thus the mGN remains the same until updating the phase variation in the final phase.

- **Time Epoch Length Calculation**

  The length of the time epoch, \( \Delta_{opt} \), determines the overall success of detecting attacks. Larger values of \( \Delta_{opt} \) tends to slow down the attack detection
process. This is owing to the convergence of a scheme on a less frequent basis causing the significant reduction of attack detection. The detector and the mGN nodes utilize fewer energy resources associated with the detection process during larger time epoch length whereas the smaller values of $\Delta_{opt}$ will lead to increased energy usage by the GN and mGN nodes. However, attack detection process has been successfully achieved which means, attack is detected before bringing significant damage to a target node is shown in equation 4.2.

$$\Delta_{opt} = \sqrt{\frac{2. (n - m) \cdot \left[ E_{elec} + \frac{E_{DA}}{2} + \epsilon_{fs} d_{mn}^2 \right] \epsilon_{mp} d_{mb}^2}{\alpha \cdot TI_e}}$$  

(4.2)

Where $\Delta_{opt}$ = Optimal length of time epoch.

$\alpha$ = application aspect value {0.0 - 1.0}.

$N$ = Number of MANET nodes.

$n$ = Number of detector nodes.

$m$ = Number of mGN nodes.

$TI_e$ = Expected Traffic Intensity (nJ/bit).

$d_{mn}$ = Average distance from detector node to mGN node (experimental).

$d_{mb}$ = Average distance from mGN node to source (experimental).

$E_{DA}$ = Data aggregation energy = 5 nJ/bit/signal.

$E_{elec}$ = Hardware energy = 50 nJ/bit.

$\epsilon_{fs}$ = 10 pJ/bit/m²

$\epsilon_{mp}$ = 0.0013 pJ/bit/m².
Pattern Learning

In this sub-phase, detector nodes are trained with patterns depicting permissible thresholds of maximum traffic flow for flowing towards the set of \( r \) selected target nodes at a given time epoch of length \( \Delta_{opt} \) is shown in equation 4.2. The patterns such as cluster based, flat and data aggregation are studies for keeping them in node monitoring phase.

Node behaviour Monitoring

In this phase, each GN node \( GN_n \) observes packets which are initiated or transited through its respective region of operation \( s^n_r \) as destined for one of the \( r \) critical target nodes. A table which stores the sub-pattern values to depict statistical features from observed traffic packets is called as a traffic observation table. The features of the table helps for depicting the intensity of traffic flow from the region of observation of a GN node towards the victim node set in a given time interval \( \Delta_i \). While completing the current time epoch \( \Delta_i \), the traffic observation table values are compared with corresponding sub-pattern values predefined and stored in the traffic threshold table. The traffic threshold table holds a set of sub-pattern values depicting the maximum number of requests receivable by a given target node \( r \), from the region of operation of a GN node, in a given epoch of time. Each GN node holds exactly \( r \) threshold sub-pattern values, one each for every target node of the network.

The process of observation by the GN nodes continues until reaching the end of the current time epoch. The fixed lengths of time intervals of this scheme facilitates the synchronization in the inter-node message exchange process. Further, consistency in the pattern reconstruction process has been achieved by having fixed length time intervals so as to maintain accuracy in the detection process. Difference in time epoch lengths causes incomplete pattern
reconstructions thus leading to reduction in the effectiveness of the attack detection scheme and increase in the false alarm rates.

**Communication phase**

The node monitoring phase gets completed with the onset of the communication phase in which each GN node $\text{GN}_n$ communicates with exactly two other adjacent nodes such as the successor ($\text{nsucc}_n$) and the predecessor ($\text{npred}_n$). This forms a dual-point linked chain of GN nodes which is referred also as the GN array and it helps to facilitate reconstruction of complete traffic patterns from individually observed sub-patterns of traffic flow. Moreover, verification of peer observations is facilitated by such chain of the GN nodes. Reconstruction of individual sub-patterns also takes place to generate a complete traffic flow pattern for each of the given target nodes $r$. A Message Authentication Code (MAC) performs authenticity check for all packets that are exchanged by the attack detection scheme. The tasks associated with MAC computation and verification is performed for verifying both the origin as well as the integrity of all messages exchanged by the GN as well as the decision-making (mGN) nodes. Each detector (GN) node shares its pair-wise distributed secret key with exactly three other nodes, namely, successor, predecessor and master GN (mGN) node. Here, the successor and predecessor nodes represent other GN nodes which are operating in the network as part of the GN array.

At each GN node, when the number of incoming requests for a particular target $r$ during the current time epoch exceeds the stored threshold value $\text{th}_r^n$ in the pattern table and similar anomalies are detected by its successor and predecessor nodes as that of its respective sub-patterns, $\text{pr}_{\text{nsucc}}$ and $\text{pr}_{\text{npred}}$, an attack will be generated by the GN node $n$ as a signal in the current time epoch. In contrast to it, a normalcy $r$ signal generated by the GN nodes implies incomplete or no-match between the observed traffic pattern and the stored pattern of anomalous behaviour for traffic destined for node $r$. As all
GN nodes involves in parallel communication, the delay in an overall communication incurred becomes minimal. After comparing the sub-pattern values with the adjacent GN nodes, the outcomes of the pattern recognition process are communicated from alternating members of the GN array to their designated mGN nodes. As there is a process of alternating communication between adjacent GN nodes of the GN array, the overall communication overhead becomes halved in terms of the energy spent with the scheme.

**Decision making phase**

The message duplication sent to the mGN nodes is avoided as the neighboring GN nodes perform alternative communicating with their designated mGN nodes in consecutive time epochs. Hence during time epoch $\Delta i_{i-1}$, GN nodes $G_{n-1}$ and $G_{n+1}$ will communicate with $M_{G(n-1)}$ and $M_{G(n+1)}$ respectively after which $G_{n-1}$ and $G_{n+1}$ will enter sleep mode during $\Delta i$, nodes and node $G_{n}$ will perform the communication. The mGN nodes are selected in view to enable connection of each of the GN nodes to an mGN node in the network. When selecting distantly placed GN nodes in a network spanning a large geographical area to operate as mGN nodes, the entire inter-connectivity among the GN-mGN node is not achieved. The missing links in the network between certain GN and mGN nodes reflects the performance of the detection scheme. It means that the false alarm rates of the scheme will be increased owing to its dependency of mGN nodes on default decision messages while avoiding the actual observation results from inaccessible GN nodes.

**Pattern Variation Recording**

In the network, the decaying energy contents of individual MANET nodes demand the reason for constant updating of pattern values stored in the Pattern Tables of GN nodes. The accuracy of the pattern recognition scheme depends on the frequency of update of the $\theta_i^n$ values. If the update rate differs
with the rate of declining energy resources of the target nodes (energy consumption rates), energy of the target nodes may get exhausted due to incoming attack traffic and become ignored by the observing GN nodes. At this phase, the pattern values are updated based on one of two approaches: a) Expected traffic inflow governing equations, and b) Actual traffic inflow-based pattern update. After confirming a successful attack r signal, the MANET nodes are warned about the malicious nodes.

**Algorithm Procedure**

**Initialization**

Selection of n GN nodes

For each GN Node n do

  Calculate k-Nearest Neighbors n

  Transmit n lists

End for

{mGN₁, mGN₂ ... mGNₘ} generated in MANET,

{q₁; q₂, qₙ} assigned to the n GN nodes

For each GN Node n do

  Generate pattern: \( p_n = p_1^r, p_2^r, \ldots p_n^r \)

End for

For each GN Node n do

  For each Target node r do

    Monitor \( S^r_n \) and Update traffic observation table locally

  End for

End for

For each GN Node n do
For each Target node $r$ do
   If traffic observation table entry for $r > \text{th}_r^n$ then
      Communicate with neighboring nodes $n_{\text{suc}} \land n_{\text{pred}}$ to
      Reconstruct sub-pattern $p_r^n$
   End if
End for

For each mGN Node $i$ do
   Cumulating of $r$ observations from $||n||$
   Generate decision signal: attack $r$ or normal $cyr$
End for

For each mGN Node $i$ do
   If attack $r = 1$
      Transmit attack $r$ to destination
   End if
End if
End for

For each GN Node $n$ do
   Update $\text{th}_n^r$
End

4.3 EXPERIMENTAL RESULTS

The experiments carried out in Network simulator (NS-2). NS-2 simulator is an open source simulation tool which helps for many routing and queueing algorithms written in C++ having an Object Tool Command Language interpreter as the frontend. Considering MANETs with dimensional area $1000 \times 1000$ m$^2$, a total of 100 nodes are initialized for the evaluation purpose.
The experimental setup is summarized in Table 4.1. The performance evaluation of the proposed Threshold based EAODV is done by comparing it with DSR, AODV and Trust based SDSR and the efficiency is determined.

**Table 4.1 Experimental setup**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Area (Size)</td>
<td>1000X1000 m²</td>
</tr>
<tr>
<td>Network Topology</td>
<td>Random</td>
</tr>
<tr>
<td>MAC Layer (IEEE Standard)</td>
<td>IEEE 802.11</td>
</tr>
<tr>
<td>IFQ Type</td>
<td>Queue/DropTail/PriQueue</td>
</tr>
<tr>
<td>IFQ Length</td>
<td>50</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>2 MB</td>
</tr>
<tr>
<td>Application Type</td>
<td>Constant bit rate (CBR)</td>
</tr>
<tr>
<td>CBR interval</td>
<td>1.0 (second)</td>
</tr>
<tr>
<td>No. of Packets</td>
<td>1500</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>620ms</td>
</tr>
<tr>
<td>Data Transfer Protocol</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>No. of Nodes</td>
<td>100</td>
</tr>
<tr>
<td>Maximum Transmission range</td>
<td>100m</td>
</tr>
</tbody>
</table>

**End-to-end delay**

End-to-end delay denoted the time needed for transmitting a packet from source to destination across a network. The transmission takes place depending on queuing and retransmission due to collision.
Figure 4.5 Comparison chart of End-to-end delay

The performance of the methodology in terms of end-to-end delay has been compared as shown in Figure 4.5. The graph is plotted with the number of nodes along the x-axis and the end-to-end delay values in milliseconds (ms) along y-axis. The graph implies that the proposed threshold based EAODV (T-EAODV) methods provides better performance in terms of end-to-end delay along with efficient detection of DDOS attack detection.

Packet Delivery Ratio

The successful delivery of ratio of packets to a destination is compared to the total number of packets that are sent.
The comparison of the proposed methodologies has been compared in terms of packet delivery ratio as shown in Figure 4.6. From the graph, it is understood that the performance of the proposed threshold based EAODV methods is better with in terms of packet delivery ratio with efficient detection of DDOS attack.

**Energy Consumption**

The average energy needed for sending, receiving or forward operations of a packet to a node in the network during the specific period of time measures the energy consumption.
Figure 4.7 Energy consumption

Figure 4.7 explains the performance comparison of the proposed methodologies in terms of energy consumption. The above graph clearly specifies that the proposed T-EAODV methods shows better performance in terms of energy consumption along with efficient DDOS attack detection.

Throughput

Throughput is an important metric to analyze network protocols and it is measures as the number of packets/bytes that are received by source per unit time.
Figure 4.8 Throughput comparison

The comparison of the methodologies in terms of throughput is shown in Figure 4.8. The graph implies better performance of the proposed T-EAODV methods with efficient DDOS attack detection in terms of throughput.

Normalized routing load

The computation of sent and forwarded DSR control packets divided by number of received data packets quantifies the normalized routing load.
Figure 4.9 Normalized routing load comparison

Figure 4.9 illustrates the comparison of the methodologies in terms of normalized routing load. The above graph implies that the performance of the proposed T-EAODV methods is better in terms of normalized routing load with efficient detection of DDOS attack.

Network lifetime

The time operated by a network until its first node or the group of nodes runs out of energy is referred as network lifetime. It can also be defines as the overall network lifetime measured by the remaining network energy.
Figure 4.10 Comparison of Network lifetime

The performance comparison in terms of network lifetime of is shown in Figure 4.10. The above graph is plotted with the number of nodes along the x-axis and the network lifetime in seconds (s) along y-axis. From the graph, it is known that the proposed T-EAODV method provides better performance with efficient DDOS attack detection in terms of network lifetime.

Packet drop rate

Packet drop is the phenomenon occurring when one or more data packets of data that travel across a network fails to reach their destination. Packet drop rate is measured as a percentage of packets lost with respect to packets sent.
The comparison of the proposed methodologies in terms of packet drop rate is shown in Figure 4.11. From the graph, it is understood that the proposed T-EAODV methods provides better performance in terms of packet drop rate along with efficient DDOS attack detection.

**Reliability**

Reliability depends on the ability of a network to perform desired operation such as “communication”. Figure 4.12 demonstrates the affiliation between the reliability on communications and the number of nodes. Threshold based AODV shows much higher reliability than trust based SDSR, AODV and DSR and it is still more efficient when there are larger number of nodes.
The relationship between the reliability on communications and the number of nodes is illustrated in Figure 4.12. Threshold based EAODV holds a high reliability value than SDSR, AODV and DSR and is relatively more efficient when there are larger number of nodes.

### 4.4 SUMMARY

The detailed description on the detection of DDOS attack in case of MANETs is provided in this chapter. The novel DDOS attack detection scheme called Threshold based EAODV DDOS attack detection has been developed in this work. The proposed threshold based EAODV DDOS attack detection scheme is employed based on the continuous monitoring of the packets sent/received by the nodes and then compared with a pre-defined threshold to detect the malicious activity. The experimental results are then compared which shows that the proposed scheme provides better results in terms of
performance parameters. It has also been concluded that the performance of the proposed Threshold based EAODV approach is better in terms of DDOS attack detection thus improving the overall network performance. The extension of this work offers scope for improving the attack detection accuracy by using hybrid optimization algorithm with MANET protocols.