Survivability in Mobile Ad hoc Networks

PhD Synopsis

For the Degree of

Doctor of Philosophy

in

Computer/IT Engineering

Submitted by:

Pimal Khanpara

(Enrollment No.: 139997107006, Batch: 2013)

Supervisor

Dr. Bhushan Trivedi

Dean

Faculty of Computer Technology, GLS University, Ahmedabad

DPC Members

Dr. Devesh Jinwala
Professor,
Dept. of Computer Engineering,
S V National Institute of Technology,
Surat

Dr. Darshan Choksi
Professor,
Dept. of Computer Science & Technology,
Sardar Patel University,
Vallabh VidyaNagar

Submitted to

Gujarat Technological University

1. Abstract

In the event of a disaster, the infrastructure of traditional communication networks can be overloaded or damaged severely. In such situations, infrastructure-less Mobile Ad hoc Networks (MANETs) [1] can provide communication services in an ad hoc manner. MANETs are challenging due to their fundamental characteristics such as dynamic topology, mobility of nodes, limited network resources and the absence of any centralized authority for network administration. Due to the mobility of nodes in MANETs, communication links may not be available after a short while and the number and identity of participating nodes cannot be assumed. MANETs use air as the communication medium and hence, wireless links available between networks nodes are not secure and susceptible to many attacks. In such environments, attackers may attempt to disrupt communication process and other network functionalities. To keep the normal operation of the network intact, researchers have proposed the idea of survivability, the ability of the network to continue functioning despite attacks and consequences of attacks.

Survivability is defined as the ability of a system to fulfil its mission in a timely manner, even in the presence of attacks, accidents or failures [3]. To apply this concept in MANETs, the requirements of survivability are defined based on the characteristics of ad hoc networks. Resistance, recognition, recovery and adaptability are the key properties of a survivable system. A survivability framework for MANETs consisting of three defense lines- Preventive, Reactive and Tolerance can be implemented taking into account survivability key properties and requirements for ad hoc networks [4]. Most of the existing survivable initiatives for MANETs either do not use all three defense lines or focus on only specific survivability properties and requirements, which makes such solutions attack or application specific [18]. Our research attempts to develop a survivability framework for general applications of MANETs. The proposed survivability framework consists of three lines of defense with all important properties and requirements of survivability. Prevention, detection, diagnosis, mitigation and tolerance of attacks are implemented as the functional blocks of the proposed survivability framework. The performance of this framework has been evaluated with a well-known routing protocol AODV and various possible forms of flooding attacks in ad hoc networks. Different parameters affecting the performance of the network are also varied in a range for assessing the effectiveness of the proposed framework. According to the results obtained, a MANET with the functionalities of the proposed survivability framework can survive the effects of attacks at a great extent if our framework is deployed.

2. Brief description on the state of the art of the research topic

Over the last two decades, researchers have proposed many techniques for securing ad hoc networks [6]. Most of these techniques either try to prevent attacks or intrusions from targeting networks and their functionalities; or they apply detection mechanisms to attempt to identify a specific type of attack. Whether these techniques are preventive or reactive, their goal is to protect ad hoc networks and their basic applications. These conventional security solutions use different mechanisms such as cryptography, path diversity protocols, designated hardware, overhearing neighbor communication and others [7]. However, such mechanisms and techniques are used for a specific security objective and thus can be effective to a given case, but inefficient to others. This limitation makes all existing security mechanisms and techniques incapable of individually securing MANETs against all types of intrusions and attacks.

Due to fundamental characteristics of MANETs and lack of general efficient security solutions, efforts have been put to design security solutions for achieving network survivability. In general, survivability is defined as the ability of a system to fulfill its goals and requirements, in a timely manner, even in the presence of attacks, accidents or failures [9]. Here, the term system has a broad meaning and can be used for characterizing networks. Security mechanisms are generally categorized into two defense lines: one preventive and another reactive [17]. Preventive security mechanisms attempt to prevent any type of attack, as firewalls and cryptographic systems. On the other hand, reactive mechanisms take actions on demand to mitigate the effects of attacks or intrusions, as intrusion detection systems (IDSs). However, preventive and reactive security mechanisms are not efficient to put all attacks and intrusions off [9], [17]. Thus, research groups have focused on building security mechanisms using the third line of defense, called intrusion tolerance (IT) [10]. The first line of defense, preventive security mechanisms are commonly implemented using various types of cryptography techniques and firewall concepts. The reactive defense line has the objective of detecting one or more types of attacks and can be implemented as point detection or intrusion detection systems [11]. To provide the essential network services in the presence of attacks or intrusions, the third line of defense must have the ability to tolerate the effects of malicious actions and for achieving that capability, techniques such as redundancy of information, content distribution and replication of data can be used [11]. In general, systems having the ability of tolerating attacks and intrusions are known as intrusion tolerant systems. Such system ability is very important and necessary for developing a

survivable system. Being a special case of dependability, survivability requires fault tolerance mechanisms in the security domain, to achieve intrusion tolerance. The major requirement of a survivable system is to provide basic functionalities and services in any case. Other important properties of survivability are resistance, recognition, recovery and adaptability. In addition to these properties, survivable ad hoc networks have system and application specific requirements.

Survivable solutions proposed for MANETs by researchers mainly consider essential services and functionalities that are required to be provided in any critical situation. Our paper [18] summarizes such existing survivability mechanisms with their properties and effectiveness. Many of these survivable solutions do not define all three lines of defense but make the use of more than one defense line and have properties needed for tolerating the effects of attacks. However, the existing survivability initiatives mainly focus on preventive and reactive defense lines and pay less attention to intrusion tolerance. Moreover, these solutions are designed for specific attacks or specific network layer functionalities. Some of the important requirements for achieving survivability are not explored yet [18]. Based on this observation, we concluded that to build a framework which proposes to provide complete survivable security solution, all defense lines need to apply cooperatively. The survivability framework should be generic and should consider multi-layer functionalities and multi-attack solutions. At the same time, the survivability framework should have the capability of adapting unexpected situations. Both these issues have been addressed in the proposed survivability framework.

3. Definition of the problem

- Developing a complete, general, routing-protocol-independent survivability framework for MANETs has been considered as a novel problem. To secure mobile ad hoc networks from different types of attacks, this framework should implement three defense lines: Preventive, Reactive and Tolerant.
- The proposed survivability framework should consist of five functional blocks: Prevention, Detection, Diagnosis, Mitigation and Tolerance. The properties and requirements of survivability are to be considered to develop the proposed survivability framework.

4. Objective and scope of work

- To use preventive and reactive defense lines for securing MANETs from attacks.

- To make networks capable of tolerating the effects of attacks and provide the essential services even when the network is under attack, however with degraded performance.
- To integrate three defense lines to develop a complete, generic and routing protocol independent survivability framework for MANETs considering properties and requirements of survivability and access the amount of fault tolerance despite attacks.

5. Original contribution by the thesis

Very less work has been done for making MANETs survivable [17][18]. Most of the existing survivability initiatives for MANETs do not define all three lines of defense and are designed for specific attacks or specific network layer functionalities. The proposed survivability framework for MANETs is generic and independent of ad hoc routing protocols. It can be integrated in existing MANETs to provide essential network services in the presence of various attacks at different network layers. The entire work presented in this synopsis is original, with research papers as the back bone. The proposed survivability framework has been visualized as a collection of five functional blocks, each of which with relevant publications. The details of the research papers are as follows:

Paper Presented / Published:

1) Security in Mobile Ad Hoc Networks. In Proceedings of International Conference on Communication and Networks (pp. 501-511), 2016. Springer, Singapore.
2) Security issues in MANETs. 3rd International Conference on Emerging Trends in Engineering, Technology, (ICETETSM-17), 2017.
3) Survivability in MANETs. International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), Vol. 7, issue 1, pp. 7-10, 2018.

Paper Submitted:

4) Survivability in Ad hoc Networks: A Review, IET Networks Journal.
5) Resisting Flooding Attacks in Mobile Ad hoc Networks, International Journal of Security and Networks, InderScience.
6) Techniques for Reactive Defense in Ad hoc Networks, International Journal of Mobile Computing and Multimedia Communications, IGI Global.
7) Intrusion Tolerance for Survivable Mobile Ad hoc Networks, International Journal of Future

Generation Communication and Networking.

6. Methodology of research, results / comparisons

6.1 Methodology of research

Qualitative, empirical and exploratory approach has been used for this research work. Several research papers and technical reports on security and survivability in ad hoc networks were studied during the literature review phase. In addition to this, different network simulators were also explored and based on our study, GloMoSim [16] simulator was chosen to implement the proposed survivability framework. It was found in literature review that existing security mechanisms for MANETs focus on either preventive or reactive defense, and fail to consider tolerance capability [17]. A few survivability initiatives proposed by researchers for MANETs are specific to attacks or network functionalities and focus on providing specific services in networks [18]. Due to these limitations, existing survivability initiatives are not generic and can be used only under certain scenarios.

Key attributes and requirements of survivability in ad hoc environments were also explored during the literature review. Based on this study and limitations of the existing survivability initiatives, it was found that to make MANETs survivable, it is necessary to use three defense lines: Preventive, Reactive and Tolerance [18]. As our aim was to develop a complete generic survivability framework for MANETs, we identified essential network services which should always be provided in any ad hoc network to complete the process of communication. The behavior of an ad hoc network is affected by the routing protocol and many times, attackers attempt to disrupt network functionalities based on routing protocol characteristics. Therefore, to make the proposed survivability framework independent of ad hoc routing protocols was also one of the objectives. Based on our study and requirements for achieving survivability in MANETs, a framework consisting of five functional blocks has been proposed. Prevention, Detection, Diagnosis, Mitigation and Tolerance are the function blocks used to implement three lines of defense. Routing and data forwarding are very important network services and should always be provided by an ad hoc network. Hence, these two essential services are considered in the design of the proposed framework. The layout of the proposed survivability framework is shown in Fig. 1. The detailed design of each functional block in the proposed framework is explained later.

To evaluate the impact and effectiveness of the proposed framework, three defense lines and their respective functional blocks are simulated individually as well as in integrated manner during

our simulation. As attackers attempt to disrupt network functionalities by targeting essential services at the network layer, various possible forms of Denial of Service (DoS) attacks have been considered in the threat model [6]. The functionalities of prevention and mitigation phases depend on the behavior of attacks and can be modified accordingly. Parameters affecting the performance of ad hoc networks in the presence of proposed framework have been varied in a range and the results are shown in section 7.

6.2 Threat Model

Denial of service attacks in MANETs are categorized as i) attacks on data traffic and ii) attacks on routing traffic [6][7]. Attacks on data traffic can be further classified into two types: i) flow disruption attacks and ii) resource depletion attacks. When an attacker corrupts, delays or drops data packets passing through it, it is called a flow disruption attack. In a resource depletion attack, an intruder seizes precious network resources such as bandwidth, energy etc. and thus these resources become unavailable for the use by the legitimate traffic in the network.

Researchers have proposed techniques to deal with flow disruption and resource depletion attacks in the ad-hoc environment. Most of these techniques rely on the design of the specific routing protocols and must be incorporated into particular ad hoc routing protocols. As we aim to build a general survivability framework, our proposed intrusion tolerance component is independent of a routing protocol and can be used with any underlying ad hoc routing mechanism.

One very popular approach to deal with flow disruption attacks is multi-path routing [14]. In multi-path routing, packets are routed along all communication paths which are available between the source and the destination. Multi-path routing uses redundancy to increase packet delivery ratio. Even if one or more paths are affected by the intruders, packets are transmitted along the other redundant paths to achieve end-to-end communication. The major downside of multi-path routing is the consumption of additional bandwidth to send packets along multiple redundant paths. Thus, the overhead in a multi-path routing protocol is usually much higher than a uni-path routing protocol. The other important drawback of multi-path routing is that conventional routing protocols for ad hoc networks do not support multi-path routing. Either they are modified to support the functionalities of multi-path routing or a new routing algorithm with the required functionalities needs to be devised.

In case of a resource depletion attack, the intruder wastes the network resources by flooding the network with spurious packets [6]. A flow of such packets drain the energy of the nodes through which they pass. A considerable amount of network bandwidth is also consumed to route such spurious traffic of packets. Intruders generate fake packets or replay legitimate packets to generate a stream of

spurious traffic. To defend the network from such resource draining attack, it is required to subdue the flow of spurious packets. The following section describes our proposed approach for defending and tolerating the impact of flow disruption and resource depletion attacks.

6.3 Proposed Survivability Framework

The layout of the proposed survivability framework is shown in Fig. – 1. This framework consists of five functional blocks: 1) Prevention 2) Detection 3) Diagnosis 4) Mitigation and 5) Tolerance

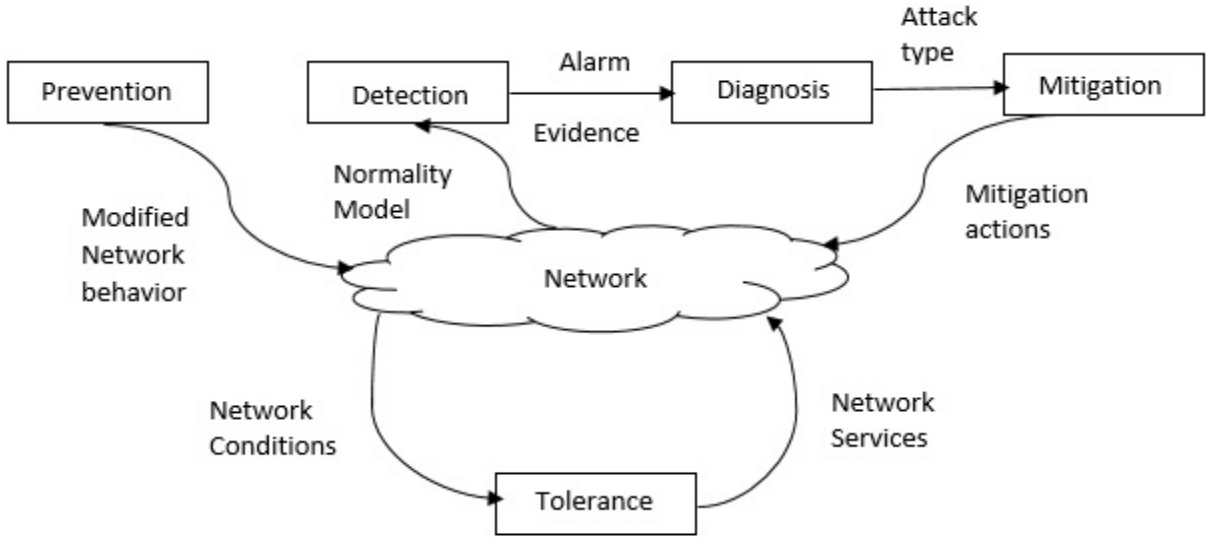

Fig. – 1 Proposed Survivability Framework

6.3.1 Prevention

In conventional networks, to prevent unauthorized traffic from entering into the network, a firewall is placed at the ingress/egress point of the network. In MANETs, the topology of the network is highly dynamic and nodes can enter or leave the network at any time. Due to these characteristics and absence of a centralized management authority, it is very difficult to define ingress/egress point for the network. Furthermore, in the ad-hoc environment, any node participating in the network could be an intruder and an attack could originate from the network itself. Hence, the conventional concept of firewalls does not work in MANETs. Moreover, traditional firewalls are not designed to resist impersonation based flooding attacks where packets are spoofed and sent as legitimate ones. Such packets can pass through the firewalls as they satisfy the access control rules mostly based on either port level or IP address level access.

Our proposal for defending MANETs from packet flooding attacks originating from the network, consists of the concept of a distributed wireless firewall. To make the firewall distributed, the functionalities of it are distributed within all nodes in the network. Each node in the network maintains an additional table, called the firewall table to maintain a list of permissible packets flows which can pass through that node. A stream of packets from one node to another is considered as a packet flow and is uniquely identified by the IP addresses of the source and destination nodes. Along with the packet flow specifications, the firewall table also maintains the thresholds for preventing a flood of spurious packets from draining the network resources. The use of these thresholds is described later in this section.

The firewall tables are not static and the entries in them are generated and maintained at runtime. This makes the design of the firewall reconfigurable. The entries of the firewall table are updated automatically to respond changes in the network topology or detected intrusions. Furthermore, the firewall table entries have finite lifetime. If the entry is not renewed within that lifetime, it is deleted from the list of permissible packet flows. There is no centralized authority in the network to manage or control the functionalities of the firewall. Thus, the firewall is configured and maintained in a completely decentralized manner.

When an intruder generates a stream of spurious traffic, the distributed wireless firewall attempts to filter out the traffic of flooding packets. As describe above, all the nodes in the network maintains a firewall table. Using the entries of these tables, the immediate one hop neighbors of the intruder prevent the attack traffic from flowing through the network and filter it out. The following paragraphs describe how this is done in our framework.

The distributed firewall is created and maintained dynamically in the network by using handshaking mechanism between the sender and receiver of a packet flow. Before initiating the transmission of data packets, the sender sends a Flow Sending Request (FSREQ) message to the receiver. The FSREQ message is sent to the receiver by using the underlying routing protocol for ad hoc networks. Upon receiving this message, if the receiver decides to accept a flow of packets from that sender, it generates a control message Flow Acceptance Reply (FAREP) and sends it back to the sender. The FAREP uses the reverse of the path taken by the FSREQ to reach the sender. Such a handshake between the sender and receiver nodes needs to be executed periodically during the lifetime of the required communication.

When an FAREP message is sent back by the receiver upon accepting the flow sending request from a sender, the FAREP message passes through the intermediate nodes. The FAREP message also contains the exact route to be followed by it. Each intermediate node on this route reads this path and creates/refreshes a time-bound entry for it in its firewall table and marks this entry as a permissible flow. Whenever handshake signals are exchanged between the sender and receiver, the entries in the firewall tables are refreshed. In case of a route failure, a new route is found according to the specifications of the underlying ad hoc routing protocol and handshaking between the sender and receiver takes place again to obtain necessary entries for the new route in the firewall tables. Firewall table entries for the flows which are no longer valid would expire and be deleted from the table.

During the reactive routing process in MANETs, intruders can exploit the routing functionality and can send a large number of route request packets. To deal with this form of flooding attacks, the proposed mechanism uses two threshold values: β and λ. The idea is to have a reasonable value of thresholds for attributes which indicate the flooding attack and raise an alarm when the attribute values cross that threshold. Initially, each node defines its default thresholds for these attributes; for all other nodes. A threshold β specifies the maximum number of packets that can be transmitted by a node in an interval and it is determined by considering average number of packets transmitted in an interval by the node and the average number of neighbors in its vicinity. γ is the maximum number of times a malicious node can exceed β before it is black listed. This threshold should not generate more false positives and thus it should be low.

If within a given time interval, a node receives more than β packets from the neighbor then the subsequent packets from that neighbor should be dropped. If the same neighbor node exceeds β transmissions by γ intervals then that neighbor node can be assumed to be flooding. All the packets received from this neighbor should be discarded in the future intervals. This technique is used for route request flooding prevention.

The other form of flooding attack can be implemented by sending a large number of fake data packets. Fake data packets do not carry any meaningful information in their payload field. To prevent this type of flooding attack, a threshold λ is used which specifies the number of fake data packets that the attacker node can send.

A destination node waits until it receives λ fake data packets from an attacker. When the number of fake data packets received exceeds λ, the destination node should broadcast that the path between it and the attacker is not available by generating an error packet. So, the path existing between

the attacker and the destination would be discarded and no new fake data packets would be sent over that path.

For each flow, the receiver monitors the duplicate packet receipt rate and the packet authentication failure rate. The proposed framework uses IPsec based packet authentication to achieve data integrity of data packets transmitted over the network. Using the packet sequence number field of IPsec header, the receiver can detect duplicate or replayed packets. The sender inserts a signed message authentication code in the authentication header field of an IP packet. Upon receiving the packet, the receiver examines this field to verify the integrity of the received message. At the receiver, impersonated or replayed packets would increase the rate of authentication failure and reception of duplicate packets, abnormally. This behavior is detected by the receiver and it is considered as an anomaly in the current flow. At that time, the receiver stops accepting Flow Sending Requests from the sender and does not send any FAREP messages over the existing path. Hence, the entries existing for this flow in the firewall tables of intermediate and source nodes would not be refreshed and would expire periodically. The sender would come to know about the path failure when it attempts to complete the required handshaking procedure with the receiver fails after a certain number of retries.

6.3.2 Detection

The detection component is implemented as a statistical anomaly detector. If the current state of the network deviates too much from the considered normal network state, this component will generate an alarm. This statistical anomaly detector needs a learning phase to derive the normality model. It is unrealistic to generate a "perfect" normality model for any network. However, to accumulate preliminary normality models, networks can be deployed in learning environments.

The basic concept of the detector is to find the deviation between the given status of the network and the normality model. The normality model is local to nodes and thus the deviation is required to be calculated for each node. At a given point in time, the state of the network perceived by a node i is represented as a state vector Si. This vector contains numerical values for selected features. The deviation can be found as the Euclidean distance $D(S_i(t))$ between the normality model local to node i and a given observation $S_i(t)$. The distance is then compared with a node-specific threshold Th_i. An alert is generated if $D(S_i(t)) > Th_i$. The threshold Th_i is generated as a part of the normality model of the node and specifies how far an observation can be from the average.

To detect an anomaly within the system, the detector needs to observe the traffic and its characteristics for a certain period of time. The alarms must be generated after that fixed time interval

if the threshold value is higher for that period. The alerts generated by the detector are processed and aggregated during the interval I_a. The number of packets evaluated and the number of alerts registered are counted during this period. The alarm is generated if the number of alerts within the given period exceeds a certain threshold Th_a. This threshold is defined in terms of proportion of alerts registered over the number of packets evaluated during I_a.

The normality model of the system is automatically generated by training the system. This model consists of four elements: the distance threshold Th_i , the maximum vector S_i^H, the minimum vector S_i^L and the average feature vector S^{avg}_i. S_i^H and S_i^L represent the maximum and minimum values observed for each feature. S^{avg}_i, S_i^H and S_i^L vectors are calculated during a period of time with a set of N observations. The maximum and minimum vectors are used for normalization (to equalize the magnitude of the different features in the vector). The normalized vector V_n at node i is calculated as $V_n = (V - S_i^L) / (S_i^H - S_i^L)$.

The distance threshold Th_i is calculated after calculating the normality vectors. To determine Th_i, the distribution of the distances $D(S_i(t))$ is characterized for a given set of M different observations. Here, to set the threshold the three-sigma rule can be applied so that most of the distributions fall inside the threshold. The range obtained using the three-sigma rule for a normal distribution covers 99.7% of the observations. Thus, Th_i is calculated as $Th_i = \mu_i + 3\sigma_i$, where μ_i is the mean distance and σ_i is the standard deviation of the given distribution.

The proposed anomaly detector uses the features which are the variables characterizing the behavior of the given system. To make this component generalized, it is required to consider the behavior of the network at routing layer. Based on the study of various ad-hoc routing protocols, following are the general features of routing layer considered which are not specific to any particular attack: Packet rates, Packet rate differences, Packet ratios, Packet distances, Number of different source addresses, Number of different destination addresses.

6.3.3 Diagnosis

The role of the diagnosis component is to identify the nature of the attack upon receiving an alarm generated by the detector component. The diagnosis is done based on the feature values that describe the node status at a given time. It is assumed that the effects of a particular attack are always of the same nature, irrespective of the network conditions and node locations.

The diagnosis component works as follows: Along with the alarm, the detector component provides the average feature vector S^{avg}_i and the status vector $S_i(t)$ as evidence. A unit length difference

vector $d_i(t)$ is then calculated as $d_i(t) = S_i(t) - S^{avg}_i$. This difference is normalized as $d_{ni}(t) = d_i(t) / ||d_i(t)||$, and called the evidence vector. To do the diagnosis, the evidence vector is required to be matched with the attack vector. It is not possible to characterize all the possible attacks during the training phase. Therefore, if an attack is not included in the attacker model and thus not known, the diagnoser component may return unknown attack as the outcome.

The attack model is composed of a number of example vectors to represent the effect of a particular attack on the different features of the status vector. As no existing dataset provides an attack model directly, an example vector for a particular attack is calculated by running a simulation in which the same is applied. To form the example vector E_j, all the observed differences across the network $d_i(t)$ are averaged and normalized (here, j is the associated attack's status and only the status vectors those were classified as anomalous are considered). The resulting attack model is a matrix $E = [E_1\ E_2\ \ldots\ E_k]$, with k columns. It is possible to characterize an attack by more than one example vectors.

To deal with non-modelled attacks, a threshold α_j is calculated for each example vector E_j. This threshold is used to determine the degree of closeness of matching attack with the given status. To calculate α_j, first all the observations used to create E_j are projected against the example vector. The distribution of projection is then studied and the threshold αj is selected as the range that contains most of the projections.

In the diagnose component, it is possible to use the same example vectors for the entire network, for every node. It is assumed that the effect of attacks is approximately uniform regardless of the normality model generated for a node.

For each interval I_a in which the anomaly detector generates an alarm, the corresponding observations are given to the diagnose as the evidence of an attack. The diagnose diagnoses each observation and the attack type associated with the largest number of observations for the given interval is selected as the output.

For each observation which is considered anomalous, the evidence vector is evaluated against the example vectors of the known attacks. The example vector that most closely resembles the evidence vector is selected as the indicator of the possible attack. The angular distance between the evidence vector and the example vector is considered as the similarity.

To determine whether the output the diagnoser is a known attack or not, a special projection vector $P_i(t)$ is calculated as $P_i(t) = E^T . d_{ni}(t)$, where E^T represents the transpose of the attack matrix. A higher projection value for a given attack matrix denotes that the observation resembles that attack most closely. The dot product between two vectors can be represented as the scalar projection of one

vector on the other. For the above dot product, the possible projection values are -1, 0 and 1 as the vectors are unit length vectors.

Let $Q_i(t)$ be the attack whose example vector has the highest projection value $P_{ij}(t)$ at node i during observation t. After selecting an example vector E_j , $P_{ij}(t)$ is evaluated against the threshold α_j. If $P_{ij}(t) >= \alpha_j$, the output is $Q_i(t)$, otherwise is unknown. At the end, all the observation diagnostics in the interval I_a are aggregated and the attack type with the largest number of observations is provided to the mitigation component. If the attack is unknown, then also the same information is given to the mitigation component.

6.3.4 Mitigation

The diagnosis component provides inputs to the mitigation component. Using this information, the mitigation component chooses an appropriate action to respond to the suspected attack. This component contains a number of mitigation actions and a mitigation controller. The mitigation controller is responsible of deciding the type of mitigation to apply and when to apply it. A generic mitigation action is applied if the detected attack is categorized as unknown.

The mitigation actions are specific to attacks. In the current proposed framework, there are two different mitigation actions specified, for flooding and wormhole attacks. The mitigation actions do not attempt to affect the attacker node's behavior or identify an attacker.

The role of the mitigation controller is to decide when to enable or disable the mitigation actions. Due to MANET characteristics and detection accuracy, it is possible that the alarms generated by the detector are not always accurate. There may exist some non-detected attack intervals while an attack is affecting the network.

The mitigation controller uses the detection rate of the diagnosed attack which is calculated during the modelling of the attacks, to extend the mitigation during a period φ after an alarm. The rate of detection is expressed as $P(D|A_j)$, which is the probability of detection provided that an attack j is present. Therefore, the probability of no detection is $1 - P(D|A_j)$. Let W be a window of a finite number of intervals during which the detector evaluations are taken. The expected number of intervals ∂ in which attacks are detected is $E[\partial] = W * P(D|A_j)$ and φ in which attacks are not detected is $E[\varphi] = W * (1 - P(D|A_j))$. Thus, the expected number of non-detections can be expressed as $E[\varphi] = E[\partial] * \{ (1 - P(D|A_j))/ P(D|A_j)\}$.

This information can be used to extend the duration of the mitigation actions after the first interval in which no anomalies are detected. Given a number of observed consecutive detection

intervals ∂, the period of mitigation is extended with φ intervals of mitigation even if no attack is detected during this time. This adaptive mitigation mechanism has two advantages: it will not mitigate for unnecessarily long periods and it will mitigate for long enough periods when the attack is ongoing. When the latest attack is categorized as unknown, the mitigation actions are not extended.

6.3.5 Tolerance

When a sender detects the failure of the current route of a flow, it invokes the overlay routing mechanism to establish a new path to the receiver. The overlay routing mechanism is independent of ad hoc routing protocols. In the overlay routing, when the sender decides to discover a new path upon inferring the failure of the existing path, it randomly selects any one node present on the current path. The selected node is called the overlay node. The sender then tunnels all packets for the destination to the overlay node, which in turn tunnels the packets received from the sender to the destination node. Thus, the path established between the source and destination nodes is an overlay path formed by linking the two tunnels at the selected overlay node. If the new overlay path consists of an intruder node (i.e., the node generating the spurious traffic) then the newly established path would fail again. In this case, the sender selects a new overlay node and attempts to reach the destination again until it succeeds or exceeds the maximum number of retries.

7. Results / Comparisons

To evaluate the performance of the proposed framework, GlomoSim (Global Mobile Information System Simulator) [16] is used. The nodes are placed using RANDOM node-placement strategy in the terrain area of 2000X2000. The traffic generator used for simulation is FTP/GENERIC and RANDOM-WAYPOINT model is used for node mobility. To show the performance of the proposed protocol, AODV routing protocol is used as an illustration.

As shown in Fig. – 2, if we vary the number of attacker nodes, keeping the number of network nodes fixed, routing overhead increases when no prevention mechanism is applied. Here, the overhead is computed in terms of number of route request packets. Without preventing the flooding nodes from generating and spreading spurious traffic flow, the attacker nodes are successful in generating a large number of route request packets in the network. The effect of applying prevention is also shown in the same graph. Overhead is reduced to a considerable amount when prevention is used.

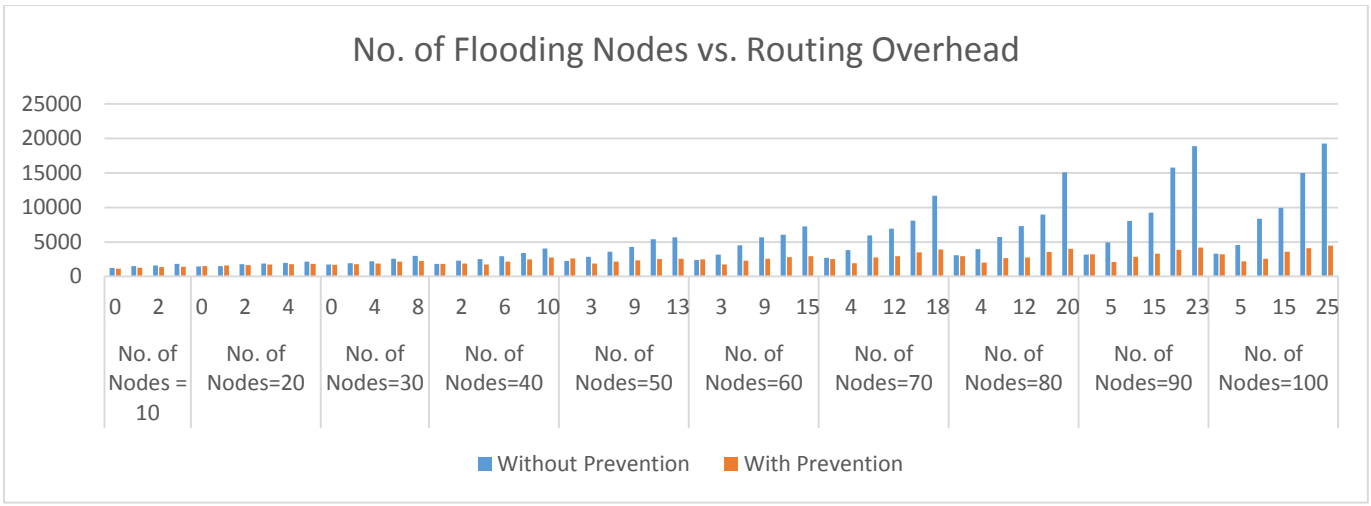

Fig. – 2 Routing Overhead

Fig. – 3 shows the effect of flooding on the number of data packets lost in the same evaluation setup. As shown in the figure, when we increase the number of flooding nodes, the rate at which data packets are lost increases. This is the case when no prevention technique is applied in the network. Due to flooding, links become congested and energy of nodes are drained. Some of the paths become unavailable due to this and hence packets transmitted over those paths are dropped. When prevention mechanism is enabled, there is a noticeable reduction in the percentage of data packets lost.

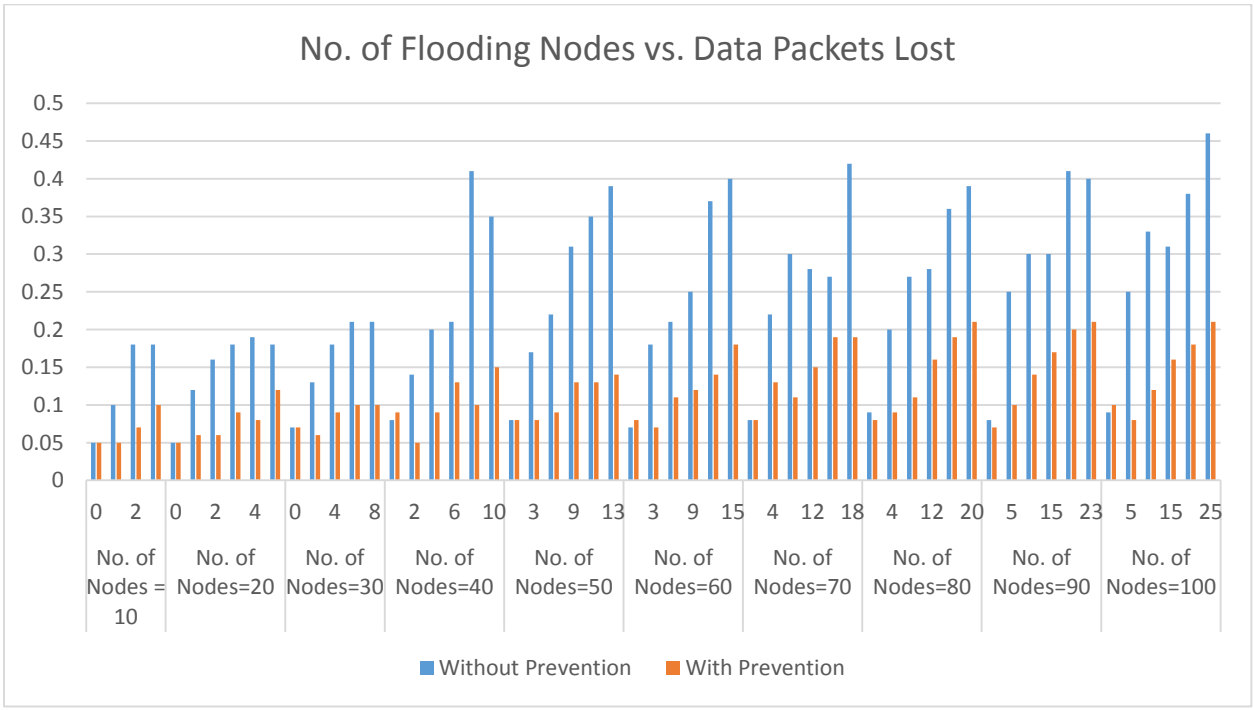

Fig. – 3 % of Data Packets Lost

To see the effects of preventive mechanism, the number of nodes and number of attacker nodes are varied in a fixed range. We assume that in any scenario, maximum 25% of the total nodes can behave as adversary. These nodes are called flooding nodes and they can launch any form of DoS attacks describe in previous sections. According to [15], the network size and the number of attacker nodes are the metrics that greatly affect the performance of ad hoc networks. As expected, routing overhead is more when preventive actions are taken. When no prevention logic is applied and the number of attacker nodes is increased, the percentage of data packets lost is very high. This percentage is significantly reduced when our approach of prevention is used.

As described in the detection phase, a normality model is needed to be derived by each node in the network. This model is based on the values contained by normality vectors computed by nodes. As AODV routing protocol is taken as an illustration, the features to be included in normality vectors are: Packet rate of RREQ, RREP and RERR packets; Packet ratios (RREQ/RREP, RREQ/RERR, RREP/RERR); number of different source addresses in received packets; number of different destination addresses in received packets. The simulation time is set to 2700 seconds, out of which first 300 seconds are used to compute node-specific normality vectors and then next 300 seconds are used to determine the distance threshold Th_i. To compute a normality vector for a node, observations are taken after varying intervals. At the time of determining Th_i, the distance values are calculated after every 60 seconds.

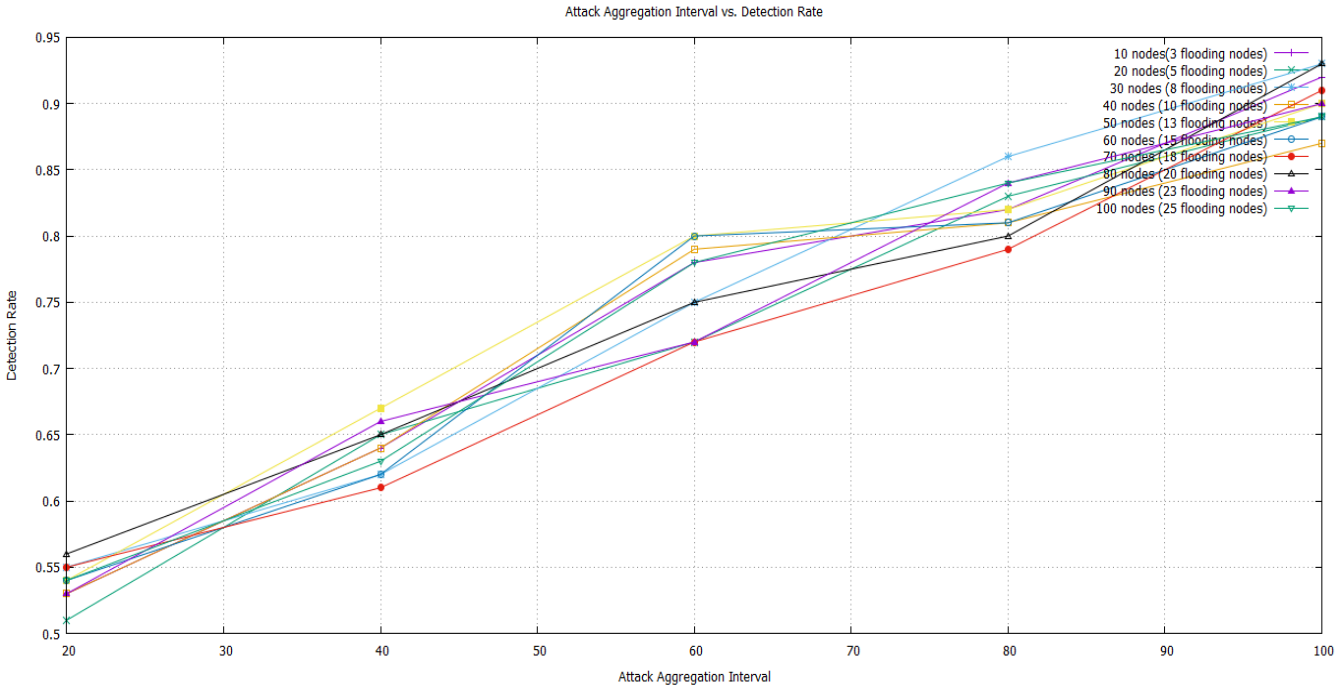

Fig. – 4 Attack Aggregation Interval vs. Detection Rate

As shown in Fig. – 4, the accuracy of the detection component is mainly based on the intervals during which observations are taken. As we increase the attack aggregation interval, detection rate improves.

Fig. – 5 shows the false positive rate calculated for the detection component varying attack aggregation interval and number of nodes and flooding nodes. With a higher aggregation interval, the false positive rate of the detection component reduces and accuracy of detection improves.

In the threat model of the proposed security framework, we consider flooding attacks. The diagnosis component of the proposed framework is able to categorize the detected attacks in two categories: Flooding and Unknown. The results of the same are shown in the Fig. – 6.

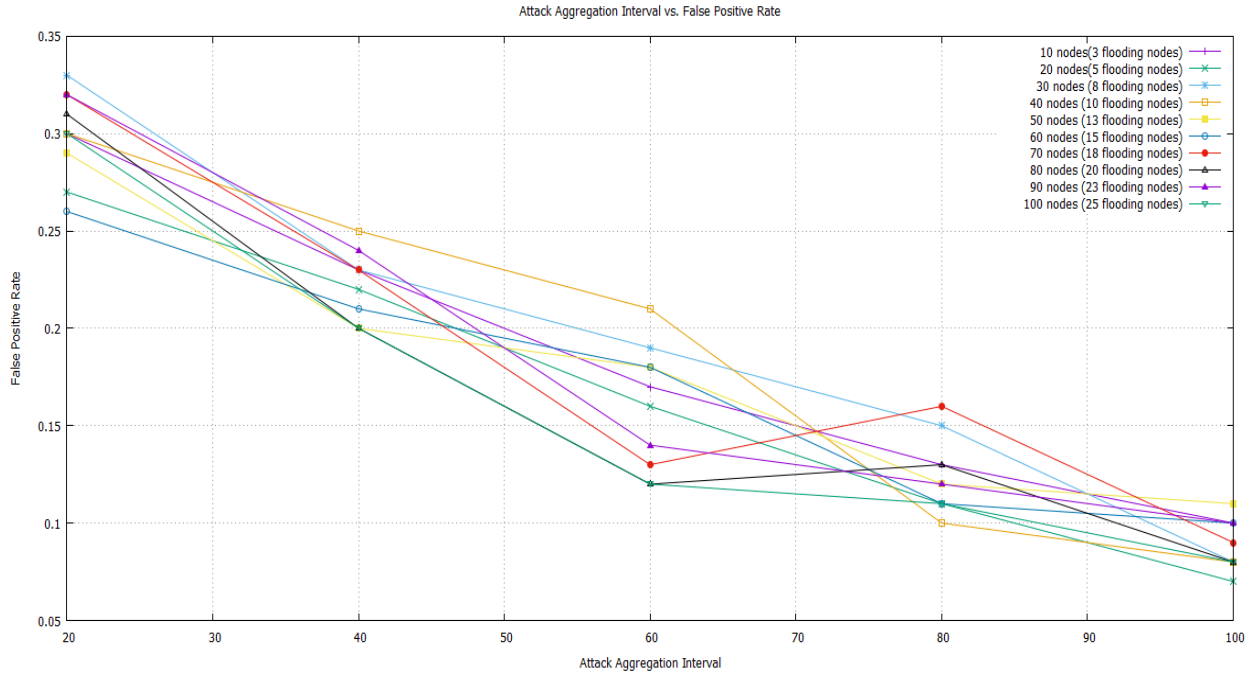

Fig. – 5 Attack Aggregation Interval vs. False Positive Rate

Fig. – 7 shows the variation in the control overhead mainly caused by routing when a range of network nodes and attacker nodes are considered in the experiment. This scenario is evaluated by varying attack aggregation interval. As attack aggregation interval has the effect on the detection component, the subsequent components also get affected by this parameter. Higher aggregation intervals improve the accuracy of detection and hence, improve the performance of mitigation component by reducing the routing overhead.

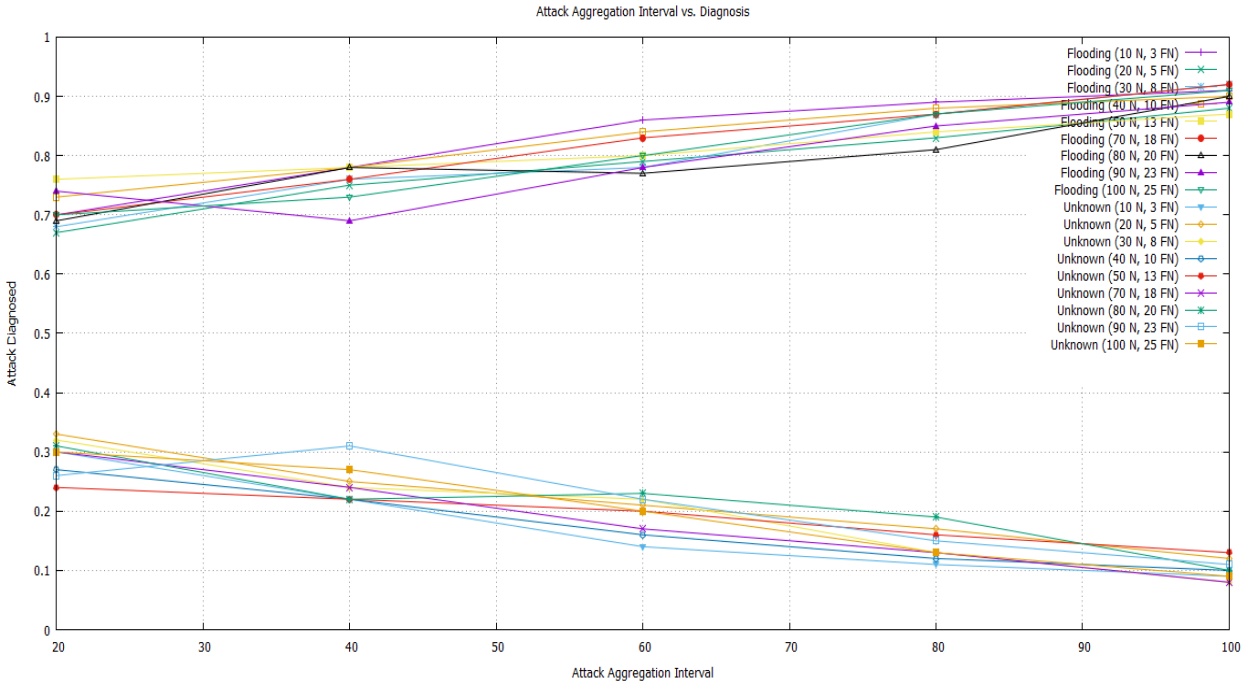

Fig. – 6 Diagnosis of attacks

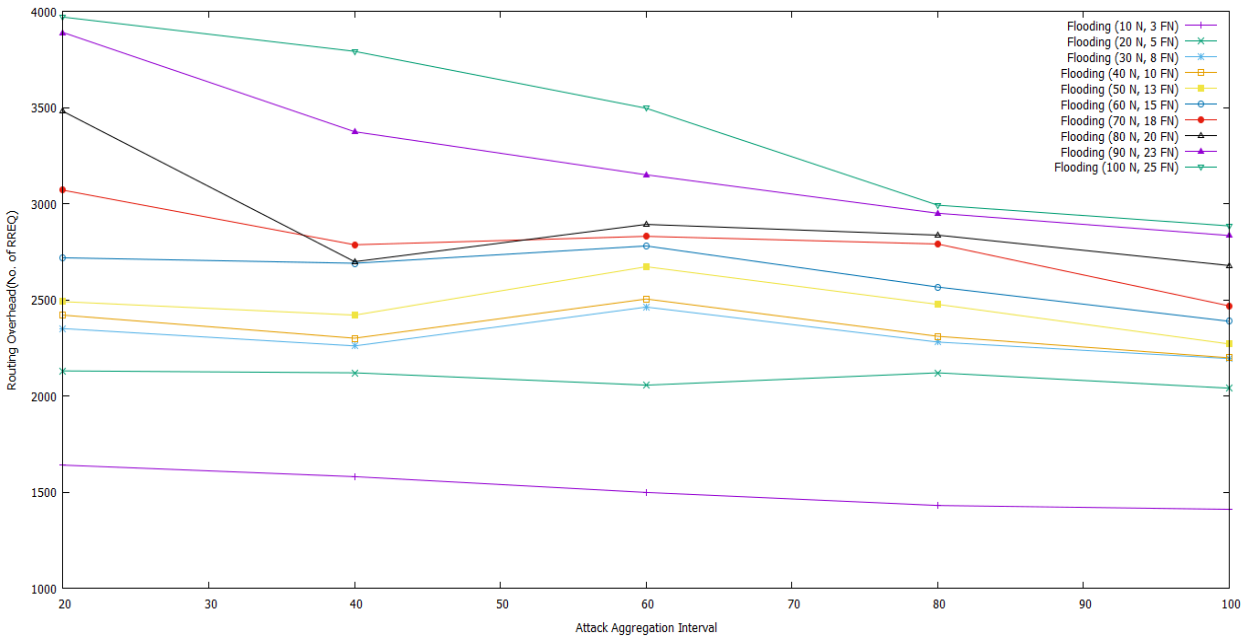

Fig. – 7 Attack Aggregation Interval vs. Control Overhead

Fig. – 8 shows the results of the mitigation component to represent the effect of different combinations of network nodes and attacker nodes on the transmission of data packets. As the mitigation component is dependent on the detection functionality, its performance is greatly affected by varying the attack aggregation interval. This graph shows that when higher aggregation intervals

are used, more attacks are detected accurately and subsequently mitigated to reduce the packet dropping rate.

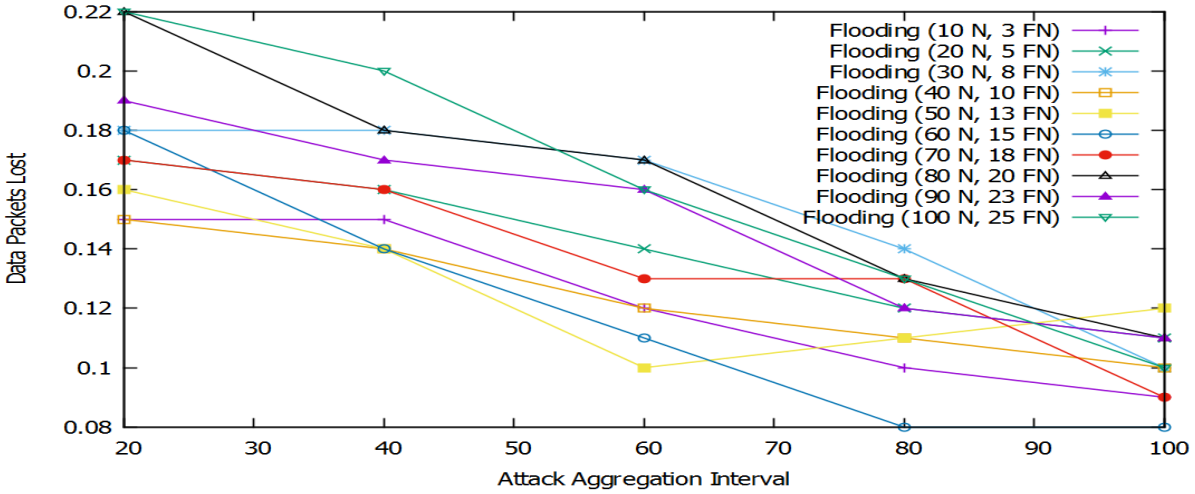

Fig. – 8 Attack Aggregation Interval vs. Data Packets Lost

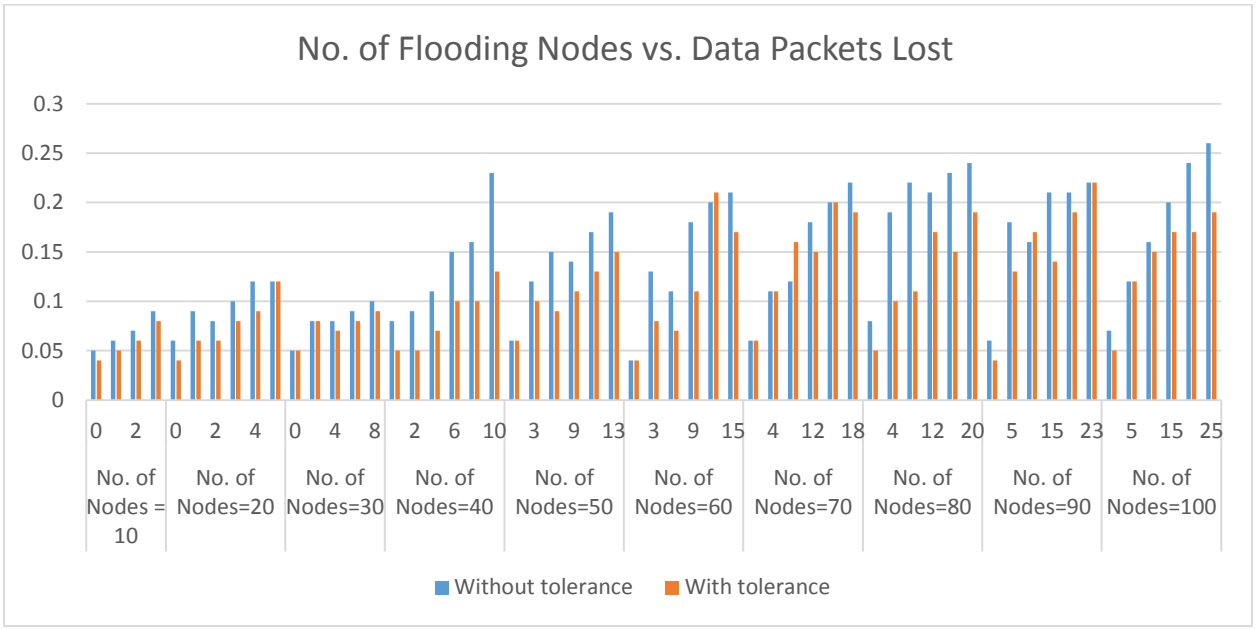

Fig. – 9 Data Packets Lost in the presence of intruder nodes

Fig. – 9 shows the effect of different combinations of network nodes and attacker nodes on the transmission of data packets. When distributed firewalls are enabled with no intrusion tolerance logic, the percentage of lost data packets increases with the higher number of attacker nodes. This percentage is significantly reduced when overlay routing is applied after detecting path failures.

Fig. – 10 shows the variation in the control overhead mainly caused by routing when a range of network nodes and attacker nodes are considered in the experiment. This scenario is evaluated with

and without applying the proposed tolerance mechanism. When tolerance component is enabled, additional control messages for periodic handshaking and overlay routing are transmitted. Hence, control overhead is slightly higher than the one obtained without applying tolerance.

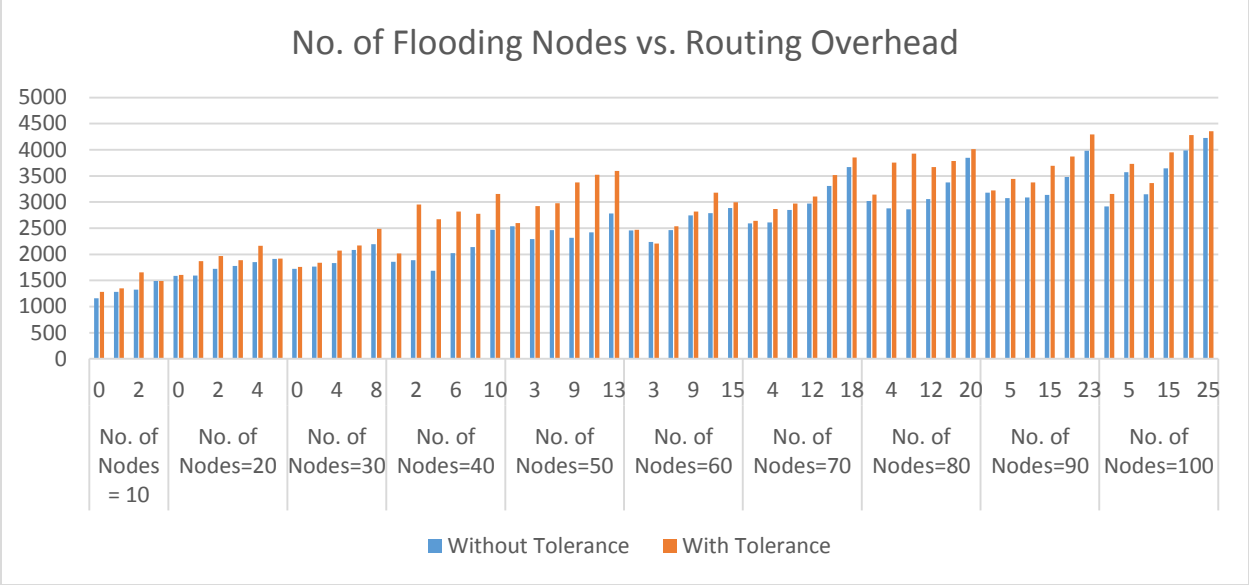

Fig. – 10 Routing Overhead in the presence of intruder nodes

8. Achievements with respect to objectives

- The outcomes of prevention, detection, diagnosis, mitigation and tolerance phases clearly indicate that our proposed framework with these phases has capability of surviving effects of attacks.
- Our framework shows considerable reduction in routing overhead, percentage of data packets lost and false positive rate. As shown in the results, rate of detection and diagnosis improves with the use of the proposed framework.
- Essential network services are always provided even if the network is under attack.
- According to the results obtained, the proposed framework outperforms the network without survivability.

9. Conclusion

Due to the increasing popularity of wireless mobile devices, the use of Mobile Ad hoc Networks (MANETs) has also increased. For most of the applications of MANETs, security is the main concern. Conventional security solutions are not sufficient to defend MANETs as they do not have tolerance capacity. The use of preventive, reactive and tolerance defense lines can make MANETs survivable. The major requirement of a survivable system is to provide basic functionalities and services in any

case. Other important properties of survivability are resistance, recognition, recovery and adaptability. In addition to these properties, survivable MANETs have system and application specific requirements. A few existing survivable initiatives are either application-specific or attack-specific and do not implement all three defense lines. Thus, a complete, generic survivability framework has been proposed to make MANETs and secure and tolerant.

According to our literature review, intrusion tolerance is almost unexplored in most of the survivability initiatives for MANETs. To implement tolerance capability, our framework focuses on essential network services which are necessary to provide even in adverse conditions. Apart from tolerance, the proposed framework has four other functional blocks: Prevention, Detection, Diagnosis and Mitigation. The simulation of all these functional phases clearly show that our framework has the capability of surviving attacks in the ad-hoc environment and provides routing and data forwarding as essential services without disruptions. The key properties and important requirements for achieving survivability in MANETs are also addressed and fulfilled in the proposed framework. The results of our experiments indicate that a MANET with our survivability framework outperforms a network without survivability. The proposed framework is generic and can be used with existing MANETs for a variety of attacks and any ad hoc routing protocol.

10. Copies of papers published and a list of all publications arising from the thesis

10.1 Paper presented / published

1) Security in Mobile Ad Hoc Networks. In Proceedings of International Conference on Communication and Networks (pp. 501-511), 2016. Springer, Singapore.
2) Security issues in MANETs. 3rd International Conference on Emerging Trends in Engineering, Technology, (ICETETSM-17), 2017.
3) Survivability in MANETs. International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), Vol. 7, issue 1, pp. 7-10, 2018.

10.2 Papers in communication

4) Survivability in Ad hoc Networks: A Review, IET Networks Journal.
5) Resisting Flooding Attacks in Mobile Ad hoc Networks, International Journal of Security and Networks, InderScience.
6) Techniques for Reactive Defense in Ad hoc Networks, International Journal of Mobile

Computing and Multimedia Communications, IGI Global.

7) Intrusion Tolerance for Survivable Mobile Ad hoc Networks, International Journal of Future Generation Communication and Networking.

References

[1] C. E. Perkins, "Ad hoc networking: an introduction," Ad hoc networking, vol. 40, pp. 20–22, 2001.

[2] P. Yi, Z. Dai, S. Zhang, and Y. Zhong, "A new routing attack in mobile ad hoc networks," International Journal of Information Technology, vol. 11, no. 2, pp. 83–94, 2005.

[3] M. N. Ahmed, H. Abdullah, and A. El-Sayed, "A Survey of MANET Survivability Routing Techniques," International Journal of Communications, Network and System Sciences, vol. 06, pp. 176–185, Apr. 2013.

[4] T. Bu, S. Norden, and T. Woo, "A survivable DoS-resistant overlay network," Computer Networks, vol. 50, no. 9, pp. 1281–1301, Jun. 2006.

[5] Y. Xue and K. Nahrstedt. Providing fault-tolerant ad hoc routing service in adversarial environments. Wireless Personal Communications: An International Journal, 29(3-4):367–388, 2004.

[6] K. Bhuvaneshwari and A. F. S. Devaraj, "Examination of Impact of Flooding attack on MANET and to accentuate on Performance Degradation," International Journal of Advanced Networking and Applications, vol. 4, no. 4, p. 1695, 2013.

[7] R. Ramanujan, S. Kudige, S. Takkella, T. Nguyen, and F. Adelstein, "Intrusion-resistant ad hoc wireless networks," in MILCOM 2002. Proceedings, 2002, vol. 2, pp. 890–894 vol.2.

[8] M. Lima, A. Santos and G. Pujolle, "A survey of survivability in Mobile Ad Hoc Networks", IEEE Communications surveys & tutorials, Vol. 11, No. 1, First Quarter, 2009.

[9] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A.W. Jackson, D. Levin, R. Ramanathan, and J. Zao. Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions. In Proceedings of ACM workshop on wireless security (WiSe), pages 31–40, New York, NY, USA, September 2002. ACM Press.

[10] N. A. Boudriga and M. S. Obaidat. Fault and intrusion tolerance in wireless ad hoc networks. In Proc. IEEE Wireless Communication and Networking Conference (WCNC), volume 4, pages 2281–2286, Washington, DC, USA, 2005. IEEE Computer Society.

[11] J. P. G. Sterbenz et al., "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," Computer Networks, vol. 54, no. 8, pp. 1245–1265, Jun. 2010.

[12] S. Y. Oh, M. Gerla, and A. Tiwari, "Robust MANET routing using adaptive path redundancy and coding," in 2009 First International Communication Systems and Networks and Workshops, 2009, pp. 1–10.

[13] J. Cucurull, M. Asplund and S. Tehrani. Surviving Attacks in Challenged Networks. IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6, pp. 917-929, 2012.

[14] R. Ramanujan, S. Kudige, and T. Nguyen, "Techniques for intrusion-resistant ad hoc routing algorithms (TIARA)," in Proceedings DARPA Information Survivability Conference and Exposition, 2003, vol. 2, pp. 98–100 vol.2.

[15] D. Perkins, H. Hughes and C. Owen, Factors Affecting the Performance of Ad Hoc Networks, In Proc. IEEE International Conference on Communications, Vol. 4, pp. 2048-2052, 2002.

[16] L. Bajaj, M. Takai, R. Ahuja, K. Tang, R. Bagrodia and M. Gerla, "GloMoSim: a scalable network simulation environment". UCLA Computer Science Department, Technical Report – 990027, May 1999.

[17] P. Khanpara and B. Trivedi, "Security in mobile ad hoc networks," Proceedings of International Conference on Communication and Networks, Springer, 2017, pp. 501-511.

[18] P. Khanpara and B. Trivedi, "Survivability in Ad hoc Networks: A Review", Submitted to IET Networks Journal.