CHAPTER 2
THE PRELIMINARIES

In ad hoc networks, wireless mobile nodes without restraint self-organize into random and momentary network topologies, allowing people and devices to internetwork in settings with no pre-existing communication infrastructure. Such type of networks is distinguished from other types of networks by its specific characteristics, vulnerabilities and application areas. Due to the vulnerable nature of these networks, these networks are more prone to attacks. This nature arise the need of supplement security measure in the existing ad hoc network infrastructure. Among the current security solutions, trust has proven its role in the enhancement of the security of the vulnerable network environments in the various areas like in social networks, ecommerce, grid computing and distributed system. The positive impact of trust in routing and authentication of ad hoc networks leads to advantage of adding trust as an integral component of the ad hoc network.

The present chapter gives an exhaustive study of ad hoc networks in terms of its characteristics, vulnerabilities, challenges, application areas, routing, authentication and attacks. The purpose of this chapter is to recognize the vulnerabilities and to identify the attacks on ad hoc networks with an aim to conclude the need of supplement security measure in the current infrastructure of the ad hoc network.

2.1 Ad Hoc Networks

The DARPA Packet Radio project which began in early 70’s established the notion of ad hoc wireless networking. DARPA had a project known as packet radio, where several wireless
terminals could communicate with one another on a battlefield. The word “ad hoc” entails that this network is customary for a special, often uttered on the spur of the moment service adapted to applications [30]. Ad hoc networks are of the interest owing to the lesser price of realization and the likelihood for mobility. The capability to swiftly set out them under both usual and unkind provisions has made it paramount in such environments.

2.1.1 What are Ad Hoc Networks?

Ad hoc networks correspond to complex distributed systems that encompass wireless mobile nodes that can without restraint and with dynamism self-organize into random and momentary, “ad hoc” network topologies, permitting people and devices to effortlessly internetwork in locales with no pre-existing communication infrastructure. An example is shown in Figure 2.1.

![Figure 2.1: A view of an Ad hoc Network](image)

An ad hoc wireless network is a network of two or more devices equipped with wireless communications and networking potential. These devices are able to commune with a further node that is instantly contained by their radio range or one that is out to their radio range. For the latter situation, an intermediate device is in role to pass on the packet from the source headed
towards destination. Such devices can take diverse forms like palmtop, laptop, mobile phone etc. The computation methodology, storage and communication capabilities of these devices will vary immensely. Ad hoc devices are not only capable of to discover the existence of connectivity with neighboring devices, but can also recognize the type of the device and their corresponding characteristics.

It is worth to mention that ad hoc networks are not an alternative or substitution of the networks with infrastructures. Their extent is in the locale where cost, environment, or application constraints require self-organized and infrastructure-less solutions [31]. Moreover the perception that a wireless ad hoc network is equivalent to a conventional tethered network except that the cables are replaced with antennas is a common misconception. Wireless ad hoc networks have unique characteristics that necessitate special solutions.

These networks are built, used, and sustained by their constituent wireless nodes over a certain geographical area. Nodes in ad hoc networks do not have a priori awareness of the topology of network. They ought to ascertain it. A node will discover its local topology by broadcasting its existence, and listening to broadcast announcements from its neighbors. With the passage of time, each node acquires to know about all other nodes and finds the ways to reach them.

An ad hoc network may be connected through dedicated gateways, or nodes functioning as gateways, to other fixed networks or the Internet. So, through this it can expand the access to fixed network services. These nodes generally have a limited transmission range and, so, each node seeks the assistance of its neighboring nodes in forwarding packets, in the case of multi hop ad hoc networks. In order to establish routes between nodes which are farther than a single hop, specially configured routing protocols are engaged. The nodes in an ad hoc network function
both as a host and router, with the control of the network distributed among the nodes. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology.

2.1.2 Networking Infrastructure

The core of the networking infrastructure is formed by the physical topology and the logical structure of the network [32].

- **Flat infrastructure (zero-tier)**
  - All nodes have equivalent routing roles
  - No hierarchy

- **Hierarchical infrastructure (N-tier)**
  - Cluster nodes have different routing roles
  - Control the traffic between cluster and other clusters

2.1.3 Characteristics of Ad hoc Networks

The characteristics of ad hoc networks are summarized [33][34][35] as follows.

- **Infrastructure-less or with minimum infrastructure support**: An ad hoc network is a group of mobile devices with a radio transmitter and receiver, coupled in short of or with a bare support of any fixed infrastructure.

- **Self-organizing and self-managing**: All interactions have to be executable in that absence of any third party support. The organization and management of mobile ad hoc network is distributed along with the participating nodes.

- **Dynamic Network topology**: Nodes in ad hoc networks are open to move randomly. The network topology may change indiscriminately and have no constraint on their distance from the rest of the nodes. Consequently, the entire topology is changing in an unpredictable way.
• **Wireless**: This type of network is wireless in nature. This characteristic of the network make it more practical but also cause complexities.

• **Node is both a host and a router**: In a mobile ad hoc network, a packet can travel from a source to a destination either directly, or through some set of intermediate packet forwarding nodes. Therefore, nodes rely on each other to established communication, thus each node as well acts as a router.

• **Multi-hop**: The nodes in this type of network have limited range. When a source node and destination node for a message is out of the radio range, it is accomplished with multi-hop routing. Because of this support communications beyond Line of Sight is possible at high frequencies.

• **Power constraint**: In most of the scenarios, ad hoc networks operate on low power devices. The battery exhausts because of added work executed by the node so as to survive in the network.

• **Low Transmission Range**: Such networks have a very limited transmission range because of the devices use radio or infrared frequencies for their communications. But this transmission range can be increased by using multi hop routing paths.

• **Low transmission Power**: There is gain in transmission power as it is required more for sending a signal over any distance in one long hop than in multiple shorter hops.

• **Variation in scale**: As the nodes are mobile in nature, so there is frequent addition or deletion of nodes in a network and hence there is variation in scale. Thus we can say that such networks have dynamic infrastructures.

• **Distributed**: For the central control of the network operations, the control and management of the network is distributed among the terminals.
• **Heterogeneity**: The participating nodes in a single network may range from mobile devices, PDAs to laptops so there is heterogeneity among the nodes.

• **Mobility**: Mobility is not, however, a requirement for nodes in ad hoc networks, in ad hoc networks there may exist static and wired nodes, which may make use of services offered by fixed infrastructure.

• **Economical**: They are economical in some cases, as they eliminate fixed infrastructure costs and reduce power consumption at mobile nodes. Moreover because of short communication links, radio emission levels can be kept low. This reduces interference levels, increase spectrum reuse efficiency, and makes it possible to use unlicensed unregulated frequency bands.

• **Robust**: They can be more robust than conventional wireless networks because of their non-hierarchical distributed control and management mechanisms.

• **Temporary**: Ad hoc networks are temporary networks because they are formed to fulfill a special purpose and cease to exist after fulfilling this purpose.

### 2.1.4 The Challenges

The ad hoc network is insecure attributable to its nature of structure. The absence of centralized machinery may reason several intricacies when there is a need to have a centralized coordinator; restricted power supply can also source some selfish problems [36]. Thus, an ad hoc network will necessitate more vigorous security design to make certain the security of it, in comparison to the wired network. An ad hoc network environment has to overcome certain issues of limitations and inefficiency [36][37] [38] summarized as follows. It includes
• **Limited range of wireless transmission** – The restricted radio band consequent in less data rates as evaluated to their counterpart, wireless networks. So best possible usage of bandwidth is obligatory by keeping minimal overhead as achievable.

• **Dynamic Nature of Topology** - The dynamic nature of network topology results in recurrent path breaks and routes often change due to mobility. Robustness of ad hoc networks in highly dynamic environments with changing load and variable speeds of the nodes is hard to achieve. Therefore, any security solution with a static configuration would not be adequate for it.

• **Recurrent network partitions** - The indiscriminate movement of nodes frequently leads to partition of the network. This typically have an effect on the intermediate nodes. The continuously changing scale of the network has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network.

• **Lack of defense boundaries**: As the nodes have freedom to join, leave and move inside the network, so there is no clear line of defense. The edges that divides the inside network from the outside world becomes fuzzy. This may cause some of the nodes may be compromised by the adversary and thus perform some malicious behaviors that are hard to detect.

• **Physical threats**: The portable devices and the system security information stored in it are susceptible to compromises or physical capture.

• **Trust on Co-operation**: The decentralized decision making in the ad hoc network relies on the cooperative participation of all nodes. The malicious node could simply block or modify the traffic traversing it by refusing cooperation to break the cooperative algorithms.
2.1.5 Vulnerabilities of Ad hoc Networks

Vulnerability is any hardware, firmware, or software flaw that can cause an information system open for potential exploitation. Among the intrinsic vulnerabilities of ad hoc networks, some reside in their routing, others in their use of wireless links and still some others in their auto-configuration mechanisms. The various vulnerabilities that subsist in the ad hoc networks are [36] [37] [39]

- **Channel Vulnerability**: The use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. The attacks can come from all directions and target at any node. An attacker just needs to be within radio range of a node in order to intercept network traffic.

- **Node vulnerability**: The nodes with inadequate physical protection are receptive to being captured, compromised and hijacked.

- **Lack of infrastructure**: The lack of centralized authority means that the adversaries can exploit this vulnerability for new types of attacks designed to break the cooperative algorithms used in ad hoc networks.

- **Dynamically varying network topology** puts security of routing protocols under threat.

- **Power and computational restrictions** prevent the use of complex encryption algorithms.

- **The self organization and management mechanism** also brings up new vulnerabilities. For example, in the case of duplicate address detection, a danger exists that a malicious node may pretend to be using any of the addresses chosen by an incoming host, thus denying the incoming host the right to join the network.
2.1.6 Application Areas

There are many areas where ad hoc networks have applications [39] [40] [41] such as

- **Military tactical operations**: In hostile or unfamiliar situations establishment of military communications can be instituted in a quick manner. The vast majority of these nodes move around at varying speeds and nodes may lose connectivity to other nodes as they move around in the battlefield because of the terrain, distance among the nodes, all these issues can also be addressed by ad hoc networks.

- **Search and rescue missions**: This can be used for search and rescue operations as communication for these may have little or no wireless infrastructure support.

- **Disaster relief operations**: During major emergencies and disasters such as hurricanes or large explosions, the communications infrastructure in the immediate area of the disaster or emergency may be unusable, unavailable, or completely destroyed. Such networks are well suited for such an application because of their ability to create connectivity rapidly with limited human effort.

- **Commercial use**: This type of network can be used for enabling communications in exhibitions, conferences, lectures and large gatherings.

- **Industrial use**: The other generally considered application for ad hoc networks is interconnection of sensors in industrial settings. Sensors are typically small devices measuring environmental inputs such as temperature, motion, light, etc. and often alerting users and/or taking specific reactions (e.g. starting an air-conditioner) when those inputs reach specific ranges.

- More recently researchers have regarded the use of ad hoc networks in the **vehicular environment**. Allowing ad hoc networking capabilities accessible in such environments
can facilitate a variety of new applications such as sharing of up-to-date traffic information among vehicles.

2.1.7 Security Goals

It is easier for hackers to snoop and gain access to confidential information. A hacker can easily enter or leave a wireless network as no physical connection is needed. They can also straightforwardly attack the network to delete messages, inject false packets, or impersonate a node. This contravenes the network’s goals of availability, integrity, authentication, and non-repudiation [37]. However for a secure networking environment, some or all of the following service are requisite [39][42][43][44][45][46][47].

- **Availability**: The goal is to ensure the availability even though Denial of Services attacks. In unreliable wireless communications with highly dynamic topology, availability affects network performance greatly.

- **Confidentiality**: The goal is keep the secret information secret. Participating parties to handle an emergency event need to cooperate with each other, while keeping the confidentiality of the traffic traversing the network. Secrecy and privacy are other terms that are considered synonymous with confidentiality.

- **Integrity**: The goal is to maintain the data integrity. The message on transmission never gets ruined or integrity should not be compromised.

- **Authentication**: The goal is to validate the node’s identity. This is by enabling a node to firm the identity of the peer node it is communicating with. Without authentication, malicious attackers can access resource, gain sensitive information, and interfere with the operation of other nodes very easily.
• **Authorization**: It is a procedure in which an entity is issued a credential, specifying the privileges and permissions it has and cannot be erroneous, by the certificate authority.

• **Anonymity**: It connotes that all the information pertaining to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software.

• **Non-repudiation**: This is the concept that ensures that the origin of a message cannot deny having sent the message. It is useful for detection and isolation of compromised nodes.

### 2.1.8 Attacks on Ad hoc Networks

An attack is an effort to evade the security controls on a computer. The attack may target to alter, release, or deny data. Attacks not in favor of the network may come from malicious nodes that are not may be the component of the network and are attempting to join the network illegitimately. The success of an attack depends on the vulnerability of the system and the efficacies of existing countermeasures. There are number of attacks that are designed to exploit the vulnerabilities of ad hoc networks.

There are broadly two types of security attacks [39][46]

• In a **passive attack**, a malicious node either ignores operations supposed to be accomplished by it or listens to the channel, attempting to retrieve valuable information. However, this process of gathering information might lead to active attacks later on.

• In an **active attack**, information is inserted to the network and thus the network operation or some nodes may be harmed.

There are two sources of threats. The first is from external attackers. Attackers could effectively divide a network by injecting erroneous routing information or distorting routing
information. They may introduce a traffic overload by causing retransmission and inefficient routing. The other type of threat comes from compromised nodes, which might misuse routing information to other nodes or act on data in order to induce service failures.

Another classification is shown in the following Figure 2.3.

![Figure 2.3: A classification of attacks](https://drachma.colorado.edu/Adhoc+Network+Security+Concerns+And+Possible+Solutions.pdf)

A number of attacks have been identified for the ad hoc networks. Some of the common known attacks found in literature are as follows [37][45].

**Wormhole Attack**

A particularly severe security attack, called the wormhole attack, has been introduced in the context of ad hoc networks. During the attack a malicious node captures packets from one
location in the network, and tunnels them to another malicious node at a distant point, which replays them locally [15]. A very simple end-to-end algorithm to handle wormhole attacks on ad hoc networks with variable communication ranges was presented [48].

**Black Hole Attack**

Black hole attack is one of these. In this type of attack, a malicious node which absorbs and drops all data packets makes use of the vulnerabilities of the on demand route discovery protocols, such as AODV. Black hole behavior may also be due to a damaged node dropping packets unintentionally. In any case, the end result of the presence of a black hole in the network is lost packets. [49]. A paper proposes a collaborative architecture to detect and exclude malicious nodes that act in groups or alone [50].

**Flooding Attack**

The data flooding attack sends many data packets in order to clog not only a victim node but also the entire network since all packets are transmitted via multiple hops. Hence, data flooding attacks are extremely hazardous to wireless ad hoc networks [51].

**Jamming Attack**

A particular class of DoS attacks called Jamming. In fact, the mobile hosts in ad hoc networks share a wireless medium. Thus, a radio signal can be jammed or interfered, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. There are many different attack strategies that a jammer can perform in order to interfere with other wireless communications [52].

**Denial of Services Attack**

The DoS attack results when the network bandwidth is hijacked by a malicious node [53]. The attacker injects packets into the network in an attempt to consume valuable network
resources such as bandwidth, or to consume node resources such as memory or computation power. So the routing tables overflow attack and energy consumption attack can be regarded as the specific instances of DoS attack.

**Byzantine Attack**

Byzantine attack It is also been called impersonation attack, in which a malicious node may impersonate another normal node and send false routing information to create an anomaly update in the routing table. Furthermore, an attacker might gain unauthorized access to resource and sensitive information [54].

**Link Withholding Attack**

In this attack, a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes [55].

**Link Spoofing Attack**

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations [55].

**Colluding Mis-Relay Attack**

In this attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in an ad hoc network [55].

**Replay Attack**

In a replay attack [56], a node records another node’s valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation.

**Rushing attack**

This is a malicious attack that is targeted against on-demand routing protocols that use duplicate suppression at each node. An attacker disseminates ROUTE REQUESTS quickly
throughout the network, suppressing any later legitimate ROUTE REQUESTS when nodes drop them due to the duplicate suppression [57].

In addition to the above listed attacks, following are the some attacks are also quoted in the literature [2][45].

- **Malign**: Watchdog and path-rater are used in ad hoc routing protocols to keep track of perceived malicious nodes in a blacklist. An attacker may blackmail a good node, causing other good nodes to add that node to their blacklists, thus avoiding that node in routes.

- **Partition**: An attacker may try to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another.

- **Detour**: An attacker may attempt to cause a node to use detours through suboptimal routes. Also compromised nodes may try to work together to create a routing loop.

- **Routing table poisoning**: The publication and advertisement of fictitious routes.

- **Packet replication**: The replication of stale packets, to consume additional resources such as bandwidth, etc.

- **Bad Mouthing Attack**: The malicious parties can provide dishonest recommendations to frame up good parties and/or boost trust values of malicious peers.

- **On-off Attack**: malicious entities behave well and badly alternatively, hoping that they can remain undetected while causing damage.

- **Sybil**: Assuming the identity of several nodes in the network.

- **Traffic Snooping**: A form of eavesdropping where the attacker reads exposed information to gain insight into a node or network’s behavior.
- **Fabrication**: an unauthorized party not only gains the access but also inserts counterfeit objects into the system.

- **Location disclosure attack**: An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios.

- **SYN flooding attack**: The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection.

- **Newcomer attack**: A malicious node may remove their bad reputation/distrust by registering as a new user.

- **Incomplete information**: A malicious node may not cooperate in providing proper or complete information. Usually compromised nodes collude to perform this attack.

- **False information or false recommendation**: A malicious node may collude and provide false recommendations/information to isolate good nodes while keeping more malicious nodes. This attack also called a black-mounting attack.

- **Spoofing** is occurred when a malicious node misrepresents its identity in the network and alters the target of the network topology that a benign node can gather.

- **Gray-hole attack**: A malicious node may selectively drop packets, as a special case of black hole attack.

- **Selective misbehaving attack**: A malicious node may selectively provide or deny proper services.

The Table 2.1 shows the layer target by some of these attacks.
Table 2.1: Attacks on Protocol Stack

<table>
<thead>
<tr>
<th>Layer</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Layer</td>
<td>Repudiation, data corruption</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>Session hijacking, SYN flooding</td>
</tr>
<tr>
<td>Network Layer</td>
<td>Wormhole, Black Hole, Byzantine, Flooding, Resource Consumption, Location disclosure</td>
</tr>
<tr>
<td>Data Link Layer</td>
<td>Traffic analysis, monitoring</td>
</tr>
<tr>
<td>Physical Layer</td>
<td>Jamming, Eavesdropping</td>
</tr>
<tr>
<td>Multi Layer attacks</td>
<td>Replay, Impersonation, DoS, man in the middle</td>
</tr>
</tbody>
</table>

2.1.9 Conclusion

A number of solutions are proposed which lessen the vulnerability of ad hoc networks to some extent [36][38][41][42][46]. One single security solution is not perfect to protect against all kinds of different attacks against a mobile ad hoc network. Therefore, there is need to apply a multi-defense security solution that offers multiple lines of defense against many different attacks. The solution relies on multiple defenses, spanning different devices and different layers in the protocol stack. Trust can be supplemented as additional security measure to offer multiple defense security solution. The appliance of trust in computing is explored in the following section to understand its effect in computing.

2.2 Trust in Computing

Trust has its appliance in diverse disciplines of the computing. Its application in various areas of computing quoted in literature is

2.2.1 Trust in Social Networks

Trust plays an important role in a web-based social network. Given the open and dynamic nature of such an online virtual community, trust evaluation relies on transitive relationships among the direct and indirect neighbors of an evaluator. Many social networking platforms have emerged on the Web, such as MySpace and Facebook. In those networks, most participants are
usually physically unknown in real life and have no prior direct interactions with each other. Trust evaluation is important as mutual trust is a prerequisite for the success of a social network, where members collaborate to achieve common objectives. Most of the traditional trust inference mechanisms are based on simple trust networks where only trust values between adjacent nodes are taken into account. The factors like social relationships, the role of a person in a specific domain, different purposes for establishing trust relations with each other, such as making friends or carrying out business are not taken into account in existing trust inference mechanisms. Reference [58] proposes the structure of complex trust-oriented social networks which address all of the above stated constraints. A novel trust inference mechanism based on Bayesian network that executes in complex trust-oriented social networks has been proposed. A transitive trust evaluation framework [59] is introduced. The inherent relationships between a trust graph and a set of relevant trust chains were studied. They analyzed the characteristics of a trust graph in terms of its capacity, degree, and completeness, proposed a model to calculate trust along a trust chain, and evaluated a trust based on a trust certificate graph. They also developed algorithms to fuse relevant trust chains to a trust graph and identify a base trust chain set.

2.2.2 Trust in E-Commerce

E-commerce is the purchase of products and services over Internet. Many Internet users are reluctant to purchase over Internet. Lack of trust is one of the most important reasons for Internet users not purchasing over Internet. The reason of lack of trust in B2C e-commerce is multiplex. First of all, consumer cannot directly interact with products and workers. The credibility of online information is doubtful and security and privacy of key information that consumer provided through Internet are also problems that consumer care about. So under great uncertainty in Internet, trust becomes one of most important factors in the development of B2C
e-commerce. A generic model of trust for electronic commerce [60] has been introduced. The basic components of the model are party trust and control trust. They argued that an agent’s trust in a transaction with another party is a combination of the trust in the other party and the trust in the control mechanisms for the successful performance of the transaction. They have claimed that this model can be used for the design of trust related value-added services in electronic commerce. The formal analysis of the understanding that is required to obtain trust in control mechanisms in electronic commerce is also given. Reference [61] introduced a trust evaluation model in which direct and indirect trust are established separately and integrated trust evaluation framework also proposed for B2C e-commerce.

Most studies and applications focus on approaches that result in a single trust value to represent the trust level of sellers or service providers. Such a simple trust evaluation method may not be able to depict the trust history exactly and may leave misleading information to service customers as the single trust value can reflect the service reputation accumulated in a certain period and thus cannot reflect the real trust status very well. To serve for this purpose a service trust vector [62] consisting of a set of values, such as final trust level, service trust trend and service performance consistency level is proposed. Service trust trend indicates that the service trust will become better or worse in forthcoming transactions. Service performance consistency level can indicate whether the service quality is being maintained at the level reflected by the final trust value, which makes sense no matter whether the trust value is low or high.

2.2.3 Trust in Grid Systems

A grid system is a dynamic and distributed environment which contains mass entities and resources, and is involved in large-scale data exchanges and resource sharing. Thus in grid system, information security is a prime concern.
Trust mechanism is a main part of grid security. A grid system adapting trust mechanism can achieve dynamic, fine-grained authorization and decision-making, which can manage entities’ security problems effectively. Because of the fuzzy nature of trust, it is more appropriate to adopt fuzzy logic to express and compute trust than adopt probabilities approach. A paper introduces fuzzy theory [63] to grid trust and proposes a novel trust model in order to better manage trust relationships between grid entities, presenting the calculation of direct and recommended trust based on fuzzy comprehensive evaluation. This paper used dynamic trust classes instead of static trust which was mostly used by the earlier papers to solve the problem caused by static trust class usage. A new behavior trust model based on fuzzy logic in Grid [64] is proposed. The direct trust matrix can be gotten by fuzzy comprehensive judgment. The formal expression of direct trust and recommend trust are also given and with it reputation can be obtained by fuzzy deriving and fuzzy combination. In the trust model based on fuzzy logic, trust in Grid can be expressed and computed appropriately, and entities in Grid can interact with other entities more securely. A two-level fuzzy trust model [65] for grid environment as well as an inter-domain access control method based on it is presented.

2.2.4 Trust in distributed networks

Security is always a challenge for wireless distributed networks. Wireless networks are prone to certain information security threats that are either unique, or more pronounced for them. This is due to the open air nature of the channel, bandwidth limitations and constantly changing topology because of node mobility. The concept of trust management i.e., establishment of trust combined with trust monitoring, can be used to mitigate the consequences of a substantial number of these threats, if not completely eliminating them.
It has been argued that using one trust component to decide on the trustworthiness of nodes in wireless sensor network is not enough and can mislead the network. Therefore, more than one component should be considered when deciding on trust. It has been proven that a trusted node from the data point of view can be distrusted from a communication point of view and vice versa. This led to the extension of the trust computational model [66] in wireless sensor networks to include both trust components - data trust and communication trust – as decisive factors regarding the trustworthiness of nodes. The results have also demonstrated that the node is very trustworthy if it is trusted by both components at the same time and, vice versa, the node is very untrustworthy if it is distrusted by both components.

A design of the trust model [67] that not only presents a trust computation mechanism but also lays the emphasis on the trust management: how to store, access and update trust value was proposed. The trust computation mechanism is completely distributed and sensitive to the deceptive peers. The trust management is also distributed and provides anonymity, reliability in the P2P systems.

A novel trust computation and management system, called TOMS [68] is also in the literature, which not only establishes the new concepts of trust and community but also includes both the trust computation model and trust management mechanism. Using the results of extensive simulations, they have highlighted the effectiveness and efficiency of trust system in comparison to other trust schemes in traditional protocols. Thus, TOMS is shown to be dynamic, distributed, and efficient, as well as sensitive to suspicious behaviors and peers.

2.2.5 Conclusion

The trust has proved its effectiveness in providing as an added security to existing environment in various disciplines of computing. As the present study is focused on ad hoc networks, so its appliance and impact in ad hoc networks are studied in the next section.
2.3 Trust in Ad hoc Networks

Trust and reputation have been recently suggested as an effective security mechanism for open environments such as the Internet, and considerable research has been done on modeling and managing trust and reputation. There is a common assumption in the routing protocols that all nodes are trustworthy and cooperative. However, the fact is different. Malicious nodes can make use of this to corrupt the network. A lot of attacks such as man-in-the-middle, black hole, DoS may be deployed to destroy the network. The nodes in ad hoc networks are not as powerful as there is no fixed infrastructure. Trust is introduced to solve the problems.

Trust is an important aspect of ad hoc networks. It enables entities to cope with uncertainty and uncontrollability caused by the free will of others. The vulnerabilities of this network force a component node in it to be cautious when collaborating/communicating with other nodes as the behaviour of nodes change with time and environmental conditions. So, establishing and quantifying behaviour of nodes in the form of trust is essential for ensuring proper operation of ad hoc networks [69]. Trust is more applicable to ad hoc networks because

- The quite dynamic nature of the ad hoc network makes it difficult to grant the behavior definitely.
- The proposition “something is good” will be changed to “I think something is good”.

The opinion is changed to subjective view from objective view [70].

A trust evaluation based security solution [11] is proposed to provide effective security decision on data protection, secure routing and other network activities. Logical and computational trust analysis and evaluation are deployed among network nodes. Each node's evaluation of trust on other nodes should be based on serious study and inference from such trust
factors as experience statistics, data value, intrusion detection result, and references of other
nodes, as well as node owner's preference and policy.

2.3.1 Trust in Routing of Ad hoc Networks

The routing of ad hoc networks has its own unique characteristics because of the structure of such types of network.

2.3.1.1 Routing in Ad hoc Networks

In ad hoc networks, nodes are not known to the topology of their networks. Instead, they have to discover it. The essential belief is that a new node may broadcast its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them. In multi-hop networks, source and destination nodes can be away from each other by multiple hops, and therefore packets may require to be forwarded by multiple nodes on the path from source to destination. This forwarding progression of packets is known as routing. The flow of data to one destination is called unicast routing. On the other hand, for multiple destinations, this flow of data is multicast routing and if all the nodes in the network are destined by the source, then these types of flows are known as broadcast routing.

An exclusive mixture of characteristics of ad hoc networks composes routing in it remarkable. First, a highly dynamic network with frequent topological changes, because of the nodes in this network is permissible to move in an unrestrained mode, cause frequent route failures. A good routing protocol for this network environment has to dynamically adapt to the changing network topology. Second, the underlying wireless channel provides much lower and more variable bandwidth than wired networks. The wireless channel working as a shared medium takes available bandwidth per node even lower. So routing protocols should be
bandwidth efficient by expending a minimal overhead for computing routes so that much of the remaining bandwidth is available for the actual data communication. Third, nodes run on batteries which have limited energy supply. In order for nodes to stay and communicate for longer periods, it is desirable that a routing protocol be energy efficient as well [34]. Thus, routing protocols must meet the conflicting goals of dynamic adaptation and low overhead to deliver good overall performance. A visualization of the classification of routing protocols of ad hoc networks with examples is shown in the Figure 2.3. The widely accepted classification of routing protocols for ad hoc networks is [71]

- **Re-active routing protocols**
  - These type of protocols do not take initiatives for finding routes.
  - The routes are established “on demand” by flooding a query regarding it.

  *Pros and cons:*
  - They do not use bandwidth except when needed to find a route.
  - The flooding process of querying for routes causes much network traffic.
  - There is initial delay in traffic.

- **Pro-active routing protocols**
  
  Every proactive routing protocol usually needs to maintain accurate information in their routing tables. It attempts to continuously evaluate all of the routes within a network. When a packet needs to be forwarded, a route is already known and can be used immediately.

  - The routes are set up based on continuous control traffic.
  - All routes are maintained all the time.

  *Pros and cons:*
  - There is constant overhead created by control traffic.
Figure 2.3: Ad hoc Network Routing Protocols [71]
- The routes are always available.
- Respective amount of data for maintaining routing information.
- Slow reaction on restructuring network and failure of individual nodes.

- **Hybrid Protocols**
  - They combine merits of both reactive and proactive protocols.
  - Normally they exploit network hierarchical structure.

2.3.1.2 Impact of Trust in Routing

Trust enhanced DSR protocol involves trust [5] in making decisions for routing. This protocol shows higher throughput, less amount of malicious drops, higher packet delivery ratio and high routing overhead as compared to standard dynamic source protocol for ad hoc networks.

A new approach based on trust based self-organizing clustering algorithm [6] is devised. They have used the trust evaluation mechanism depending on the behavior of a node towards proper functionality of the network. As the trust value of a particular node depends on its participation towards proper functionality of the network, each node must cooperate and the network can be prevented from inside malicious attacks. They are not only restricting to direct observation for predicting trust but also recommendation from one hop neighbors of any node under review. It combines different metrics for quantifying trust and the use of Dempster-Shafer theory in order to predict the trust of mobile node more accurately.

Reference [8] protocol TAODV extends the widely used AODV routing protocol and employ the idea of a trust model to protect routing behaviors in the network layer of MANETs. In the TAODV, trust among nodes is represented by opinion, which is an item derived from subjective logic. In TAODV after the trust relationship establishment, the subsequent routing
operations can be performed securely according to trust information instead of certificates all the time. The design will detect nodes’ misbehavior finally and reduce the harms to the minimum extent. When a good node is compromised and becomes a bad one, its misbehavior will be detected by its neighbors. Then with the help of trust update algorithm, the opinions from the other nodes to this node will be updated shortly. Thus this node will be denied access to the network.

One routing algorithm [12] basically behaves depending upon the trust one node has on its neighbor. The trust factor and the level of security assigned to the information flow decide what level of encryption is applied to the current routing information at a source/intermediate node. In other words, above a certain level of trust level, there is no need for the source/intermediate node to perform high level encryption on the routing information as it completely trusts the neighboring node. So based on level of trust factor, the routing information will be low-level, medium level, high level encrypted. This not only saves the node’s power by avoiding unnecessary encoding, but also in terms of time, which is very much valuable in cases of emergencies where the information is as valuable as the time.

A new trust evaluation scheme based on clustering [13], in which a cluster is built by neighboring nodes, and a cluster head elected by cluster members acts as a trust guarantor. In our scheme, the trust of a node is evaluated by combining the node’s own experience and the information presented by the head of the cluster to which the evaluated node belongs. Even in a case when a node has no experience, it can evaluate other nodes based on the trust value provided by the cluster head. To defend against black hole attack trust guarantor of the malicious node will set a low trust value for the malicious node. Therefore, the node that wants to send a packet will discard the routing path that goes through the malicious node. A selfish node that is a
node doesn’t route a packet from the other nodes or simply drops some packets to save their power or other energy cannot have a high trust value because of the data delivery rate. By not providing packet forwarding for low trusted nodes, a network can encourage cooperation and reduce selfishness. By referring to the trust value certified by the cluster head, a node can evaluate the trust value of the unfamiliar node in spite of the absence of direct experience about the node.

An information theoretic framework [14] to quantitatively measure trust and model trust propagation in ad hoc networks is anticipated. In the proposed information theoretic framework, trust is a measure of uncertainty with its value represented by entropy. Axioms are developed that address the basic rules for trust propagation. Based on these Axioms, two trust models are presented: entropy-based model and probability-based model, which satisfy all the Axioms.

A secure routing solution [15] to find an end-to-end route free of malicious nodes with collaborative effort from the neighbors is projected. They have extended the solution to secure the network against colluding malicious nodes. Any malicious entity, trying to inject wrong routing information either independently or acting in collusion, is effectively singled out. They have also proposed a model for computing, distributing and updating trust information in the network that analyzes different malicious behavior reflecting each behavior in the model.

A comprehensive mechanism for discovering the most secure and shortest paths [16] is proposed. This proposed mechanism is based on the Dijkstra algorithm, and regards distance weight and trust weight highly. The metric value which can determine the routing path is to be extracted from the distance value and the trust level. Even though the proposed mechanism works with the trust weight as well as the distance weight, it does not make any differences in a viewpoint of the number of hops, except for raising the communication cost slightly.
Discovering the shortest secure paths in ad hoc networks by using the proposed mechanism, basically prevents internal malicious nodes from attacking or disguising, such as in the case of a wormhole.

The expansion of relevant fuzzy logic concepts to propose an approach [17] to establish quantifiable trust levels between the nodes of ad hoc networks. These trust levels approach show significant improvements in the performance and the reliability of ad hoc networks in the presence of malicious nodes. For instance, the Overall Performance Index for the fourth scenario improved by 18.91% after applying the fuzzy trust based approach where Overall Performance Index is defined as a weighted sum of the throughput, round trip delay and packet loss parameters. A trust model based on the human concept [22] of trust focus on providing nodes with a trust level for each direct neighbor, that is, neighbor within the radio range. The goal is to make nodes capable of gathering information to reason, learn, and make their own decisions. They also introduce the concept of relationship maturity. This work improves scalability by restricting nodes to keep and exchange trust information solely with direct neighbors. The results show that the maturity relationship improves the system performance allowing a higher mobility.

Trust Enhanced security Architecture for MANET [72], in which a trust model is overlaid on the following security models - key management mechanism, secure routing protocol, and cooperation model. The result confirms that SMRTI enables TEAM nodes to establish valid routes, despite the increasing proportion of malicious nodes. It is also shown that TEAM nodes exhibit improved performance in comparison with DSR nodes. However, in the presence of 90% packet dropping nodes, the performance of TEAM nodes reduces significantly when compared with DSR nodes. Table 2.2 summarized the effects of trustworthiness in the performance of routing in the case of ad hoc networks.
<table>
<thead>
<tr>
<th>Contribution</th>
<th>Key points</th>
<th>Impact on Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Based Clustering and Secure Routing Scheme for Mobile Ad hoc Networks [6]</td>
<td>Trustworthiness is by direct interactions, interactions of neighbors and recommendations.</td>
<td>Stimulates the cooperation between nodes, prevention from inside malicious attacks</td>
</tr>
<tr>
<td>A Trust Model Based Routing Protocol for Secure Ad Hoc Networks [8]</td>
<td>Extend basic AODV routing protocol, trust is obtained by opinion, dynamically modify trust value</td>
<td>More secure routing, detect bad nodes, easily adaptable to behavior and topology</td>
</tr>
<tr>
<td>Trust based Adaptive On Demand Ad hoc Routing Protocol[12]</td>
<td>Trust is based upon a node has on its neighbor, different trust level defined and security is applied accordingly</td>
<td>Highly secure, save node’s power and even the time for communication is less</td>
</tr>
<tr>
<td>Cluster-Based Trust Evaluation Scheme in an Ad Hoc Network [13]</td>
<td>Neighboring nodes form a cluster, Trust is evaluated by node own experience and the trust presented by its cluster head.</td>
<td>Defend black hole attack, detection of selfish node, perform well for strangers</td>
</tr>
<tr>
<td>Trust modeling and evaluation in ad hoc networks [14]</td>
<td>Trust is a measure of uncertainty with its value represented by entropy.</td>
<td>Improve throughput, defend gray hole attack, detect malicious nodes</td>
</tr>
<tr>
<td>Towards Designing a Trusted Routing Solution in Mobile Ad Hoc Networks [15]</td>
<td>Presents a model for computing, distributing and updating trust</td>
<td>Very good against colluding malicious nodes</td>
</tr>
<tr>
<td>Collaborative Trust-Based Shortest Secure Path Discovery in Mobile Ad Hoc Networks [16]</td>
<td>A mechanism is based on the Dijkstra algorithm, regards distance weight and trust weight highly</td>
<td>Discover shortest secure path, prevents attacks form internal malicious nodes like wormhole attack</td>
</tr>
<tr>
<td>Fuzzy Trust Approach for Wireless Ad hoc Networks [17]</td>
<td>Fuzzy logic is extended to establish quantifiable trust levels between the nodes</td>
<td>Improvement in reliability, higher throughput, lower round trip time</td>
</tr>
<tr>
<td>Analyzing a Human-based Trust Model for Mobile Ad Hoc Networks [22]</td>
<td>Provides trust level for nodes within radio range, concept of relationship maturity</td>
<td>Improves scalability, improves system performance allowing higher mobility</td>
</tr>
<tr>
<td>Trust Evaluation based Security Solution in Ad hoc Networks [11]</td>
<td>Trust is based on experience statistics, intrusion detection results, reference of other node, owner’s preference and policy</td>
<td>Defend black hole, denial of services, routing table overflow, energy-consumption attacks</td>
</tr>
<tr>
<td>TEAM: Trust Enhanced Security Architecture for Mobile Ad hoc Networks [72]</td>
<td>A trust model is overlaid - key management mechanism, secure routing protocol, and cooperation model.</td>
<td>Establish valid routes, improved performance in comparison with DSR nodes, against flooding nodes</td>
</tr>
</tbody>
</table>
2.3.2 Trust in Authentication in Ad hoc Networks

Authentication in ad hoc networks is also prone owing to the vulnerabilities of ad hoc network.

2.3.2.1 Authentication in Ad hoc Networks

Authentication is a phase of communication network security procedure to ensure that the principals with whom one interacts are the expected ones. Granting resources to, obeying an order from, or sending confidential information to a principal of whose identity we are unsure is not the best strategy for protecting availability, integrity and confidentiality [73]. Authentication [74] is a process that involves an authenticator communicating with a supplicant using an authentication protocol to verify credentials presented by the supplicant in order to determine the supplicant’s access privileges. A Trusted Third Party may be involved as part of the authentication protocol.

The supplicant is an individual or an entity that is with the purpose of to have access to any protected resources is being authenticated through an authenticator. An authenticator is an entity that is meant for protecting and controlling access to some resources. The authenticator carries out the course of authentication and makes decisions of authentication. An authentication protocol is a sequence of message exchanges between supplicant(s) and authenticator(s) that either distributes secrets to some of those principals or allows the use of some secret to be recognized. A supplicant is authenticated by an identifier known as credential. Lastly, a Trusted Third Party is an entity that is commonly having faith by the supplicant and the authenticator and that can accomplish mutual authentication between the two parties. The provisions of entity authentication and authenticated key establishment among nodes are together target intents in securing of ad hoc networks [75]. Some of the examples of authentication protocols are ARAN.
(Authenticated Routing for Ad hoc Networks), Ariadane, LHAP (Lightweight Hop-by-hop Authentication Protocol) and SAR (Security-aware Ad hoc Routing).

**Classification of authentication Protocols**

An authentication protocol is classified as per the following classification [74]

- **Homogeneous vs. Heterogeneous**: based on the roles assigned to nodes in the network with respect to the authentication operation.

- **Possession vs. Context**: identifies the supplicant based on a unique possession, while the second class identifies the supplicant based on context.

- **Prior vs. Post node deployment**: Some protocols establish credentials prior to node deployment, while other protocols assume credentials are established post node deployment.

**2.3.2.2 Impact of Trust in Authentication**

A novel trust and reputation management scheme [7] that can protect the security of transacting entities is proposed. The scheme uses a localized trust and reputation management strategy, hence avoiding network-wide flooding. The approach enables each node in the network to establish a trust value with other interacting entities with minimal communication cost and acquisition latency. The experimental results show that the scheme provides minimal overhead and can be adequately adopted for wireless sensor networks.

A security architecture [9] that extends the traditional PKI model, assigning variable trust values to digital certificates and issuing credentials to grant access to network services. Trust values are not static. Depending on the seriousness of the incidents the trust value associated to the offender’s certificate will vary.
A secure public key authentication service based on trust model [10] and network model to prevent nodes from obtaining false public keys of the others when there are malicious nodes in the network is existed in literature. The experimental results indicate clear advantages of our approach in providing effective security in ad hoc networks.

Reference [20] introduces a novel delegation system that describes digital trust between users by means of cryptographically secured tokens. The delegation system is organized by the users themselves in a fully distributed manner. The system supports anonymity, provides a high usability. The described architecture allows an anonymous propagation of tokens without the need of a public key infrastructure, which is a novelty. The user is not confronted with authentication, tokens can be passed on even if communication with the system itself is not possible and unknown users and devices are supported. Permissions of a token can be restricted and the integrity of the trust chain can be checked by cryptographic measures. To increase the controllability of the system and to motivate users not to abuse the trust someone gave them, an optional permission update list can be established.

A scheme for the distribution of trust certificates [76], which is completely distributed and adaptive to mobility, is formulated. The scheme is based on the swarm intelligence paradigm, which has been used for routing both in wired and wireless networks. The advantages are its adaptability to network changes and tolerance for the faults in networks. Moreover, because of flexibility of metrics in the reinforcement rule, it is easy to embed security and trust content in the certificate distribution process. The objective is to properly and efficiently distribute evidence in the wireless ad hoc network, which facilitates the evidence requests and reduces the communication cost. Performance results in autonomous, decentralized and mobile systems are promising.
A Key Management System [77] uses a modified hierarchical trust Public Key Infrastructure model in which nodes can dynamically assume management roles. A novel behavior grading mechanism provides security criteria for the network nodes and aids the management functions of the KMS to revoke or reissue certificates for nodes. This mechanism is based on the notion of trust, and more specifically on Security Associations among nodes in the entire network. This KMS increases service availability for all nodes, increases flexibility in accommodating new nodes, minimizes pre-configuration, and can dynamically reconfigure itself based on the network environment.

Table 2.3 provides an overview about its effectiveness at authentication.

<table>
<thead>
<tr>
<th>Contribution</th>
<th>Key Points</th>
<th>Impact on Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust-based security for wireless ad hoc and sensor networks [7]</td>
<td>enables node to establish a trust value with other at minimal communication cost and acquisition latency</td>
<td>Minimal overhead but more secure and less expensive in terms of time and cost</td>
</tr>
<tr>
<td>Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks [9]</td>
<td>Extends the traditional PKI model, assigning variable trust values to digital certificates and issuing credentials to grant access to network services</td>
<td>Highly secure authentication</td>
</tr>
<tr>
<td>An Authentication Service Based on Trust and Clustering in Wireless Ad Hoc Networks [10]</td>
<td>A public key authentication service based on trust model and network model to prevent nodes from obtaining false public keys of the others</td>
<td>Effective security, more powerful authentication</td>
</tr>
<tr>
<td>A Trust Based Delegation System for Managing Access Control [20]</td>
<td>describes digital trust between users by means of cryptographic tokens, system supports anonymity</td>
<td>supports anonymity, high usability, allows an anonymous propagation of tokens</td>
</tr>
<tr>
<td>Ant-Based Adaptive Trust Evidence Distribution in MANET [76]</td>
<td>Scheme is based on the swarm intelligence paradigm,</td>
<td>Adaptability to network changes, efficient distribution of certificate for authentication</td>
</tr>
<tr>
<td>A Framework for Key Management in Mobile Ad Hoc Networks [77]</td>
<td>A mechanism provides security criteria and aids the management functions to revoke or reissue certificates for nodes</td>
<td>Ensure high service availability, increases flexibility in accommodating new nodes</td>
</tr>
</tbody>
</table>
2.3.3 Trust in Access Control

Most ad hoc networks do not implement any network access control, leaving these networks vulnerable to resource consumption attacks where a malicious node injects packets into the network with the goal of depleting the resources of the nodes relaying the packets. To prevent such attacks LHAP [21] is a hop-by-hop authentication protocol for ad hoc networks. LHAP resides in between the network layer and the data link layer, thus providing a layer of protection that can prevent many attacks from happening, including outsider attacks and insider impersonation attacks.

A distributed mechanism that allows trusted nodes to create protected networks [78] in MANETs exists. A protected network is created to run a specific application and enforce a common network access control policy associated with that application. To become a member in the protected network, a node has to demonstrate its trustworthiness by proving its ability to enforce policies. Attacks from un-trusted nodes are impossible because these nodes are not allowed to establish wireless links with member nodes. Attacks from member nodes are stopped at the originators by the network policy. The trusted execution of all programs involved in policy enforcement is guaranteed by a kernel agent. They demonstrated the correctness of their solution through security analysis and its feasibility through a prototype implementation tested over an IEEE 802.11 ad hoc network.

There is an increasing need to secure the information collected from the pervasive computing environments, and yet to be able to allow flexible data sharing to facilitate problem-solving and decision-making. The work [79] investigates the two seemingly contradictory factors, secures access and flexible adaptation, and designs a trust inference model for emergency and crisis situations. He describes an ad hoc trust inference model where access
decisions are adaptive to the identity, history, and environment of a requester, for example, the degree of urgency. The trust inference model is built on fuzzy logic. The sharing control mechanism can also be applied to protect personal data and used for digital identity protection.

Table 3.3 shows trust consequence for access control in ad hoc networks.

Table 3.3: Impact of Trust in Access Control

<table>
<thead>
<tr>
<th>Contribution</th>
<th>Key Points</th>
<th>Impact on Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>LHAP: A Lightweight Network Access Control Protocol for Ad hoc Networks [21]</td>
<td>resides in between the network layer and the data link layer, thus providing a layer of protection</td>
<td>prevent many attacks, including outsider attacks and insider impersonation attacks</td>
</tr>
<tr>
<td>Trusted Application-Centric Ad hoc Networks [78]</td>
<td>a node has to demonstrate its trustworthiness by proving its ability to enforce policies</td>
<td>Attacks from un-trusted nodes are impossible and from bad member nodes are stopped at the originators</td>
</tr>
<tr>
<td>An Ad Hoc Trust Inference Model for Flexible and Information Sharing [79]</td>
<td>an ad hoc trust inference model where access decisions are adaptive to the identity, history, and environment</td>
<td>secures access and flexible adaptation</td>
</tr>
</tbody>
</table>

2.3.4 Conclusion

It is concluded that usage of trust as supplementary security measure for various network activities of ad hoc network has been proved to very effective. This is also revealed from the literature that the studies use trust as a foreign component to the ad hoc network environment. The trust modeling is hard-coded into that component. This approach can raise the issues like inflexibility, dependency, and non-scalability. Keeping these issues in mind we are going to develop a framework with a layered approach. In this approach one layer is independent of the other so flexibility can be achieved and dependency can be avoided. Moreover we will develop a trust model that exhibits the properties of dynamicity, subjectivity, context dependency of trust and also it will be scalable. So the inclusion of trust as an integral component in ad hoc network environment will prove to be very effective.
2.3 Summary of the Chapter

In the absence or little of pre-existing communication infrastructure, mobile ad hoc network allows wireless mobile nodes to self-organize into random and momentary network topologies. These networks made a distinction from other types of networks by its specific characteristics, vulnerabilities and application areas. The ad hoc network is prone to number of attacks. Therefore, there is need of some supplementary security measure to enhance the security of ad hoc networks to offer multiple lines of defense. Moreover, the use of trust to serve as supplement security measure is also concluded.

The next chapter presents the review of literature regarding the concepts of trust and other literature that leads us the directions for the development of the framework under study.