CHAPTER 1

INTRODUCTION

This chapter presents basic details of wireless ad hoc networks and emphasizes the need for optimal secure routing in infrastructure based wireless mesh networks. A brief review of literature pertaining to the present work is also presented.

1.1 WIRELESS AD HOC NETWORKS

Wireless ad hoc network is a kind of multi hop wireless network, making use of radio signals to communicate among the nodes in the network without using any infrastructure. Due to the wireless nature, it overcomes most of the limitations of traditional wired networks (Pietro et al. 2014). The nodes in the network are mobile and cooperate with each another for better communication in the network. Each mobile node operates not only as a host but also as a router that forwards packets on behalf of other nodes (Deng et al. 2002). Due to the inherent characteristics of wireless ad hoc networks such as dynamic topology, limited channel capacity, power constraints, open shared medium and wireless transmission impairments, the network is more vulnerable to active attacks as well as passive attacks. Hence designing an effective routing protocol for ad hoc network still remains as a challenging task. The applications of ad hoc networks range from military operations, emergency disaster recovery, community networking and ad hoc interaction meeting among persons in a conference hall. For these types of applications, security provision in the routing protocol is necessary to guard against attacks caused by internal attacks and external attacks (Pietro et al. 2014). Wireless ad hoc networks are classified into three types based on the applications: Mobile Ad hoc Networks (MANET), Wireless Mesh Networks (WMN) and Wireless Sensor Networks (WSN). In this thesis work, we address the issues of security, privacy and routing in Wireless Mesh Networks (WMN).

1.2 WIRELESS MESH NETWORKS

Wireless Mesh Networks (WMN) is an emerging wireless technology for next generation wireless networking and it plays a crucial role in offering real-time services for the applications running on the networks. It is a multi hop wireless network that consists of Mesh Routers (MRs), Mesh Gateways (MGs) and Mesh Clients (MCs). Mesh Routers are typically stationary and form the fixed wireless infrastructure (backbone) of WMNs. Mesh Clients access the network through the mesh backbone of the WMN. In mesh backbone, some MRs act as gateway nodes to connect with the other external networks such as the Internet, cellular and sensor networks, etc. The network is dynamically self-organized, self-configured and the nodes within the network automatically formulate and preserve the mesh connectivity among themselves (Akyildiz et al. 2005, Nandiraju et al. 2007). Besides this, WMN has more advantages like low installation cost, simple network maintenance, robustness and reliable service coverage. Based on the network architecture, WMNs are classified into three types as discussed in Akyildiz et al. (2005): Infrastructure based WMNs, Client WMNs and Hybrid WMNs. We have considered infrastructure based WMNs to implement our proposed work.

Infrastructure or Backbone based WMNs

In this type of WMNs, backbone is formed by mesh routers and mesh clients. Mesh clients are connected to any one of the nearest edge mesh router. To build infrastructure or mesh backbone, different types of radio technologies are used in addition to IEEE 802.11 technologies. Each mesh router has self configuring and self healing capability. To connect with the Internet or any other external networks, some of the mesh routers in the backbone act as gateway nodes. Hence, mesh routers provide an infrastructure or a backbone for conventional clients to access the network and also for communicating with other external networks such as cellular network, sensor network, Wi-Fi and WiMax networks, etc (Akyildiz et al. 2005). The most commonly used type is infrastructure based WMNs which is shown in Figure 1.1. In this thesis, the proposed work is applied in infrastructure based WMNs. The physical protection of mesh routers is very weak since they can be placed on the roof of houses in the neighborhood to serve as access points for users in the community and neighborhood networks (Martignon et al. 2011).

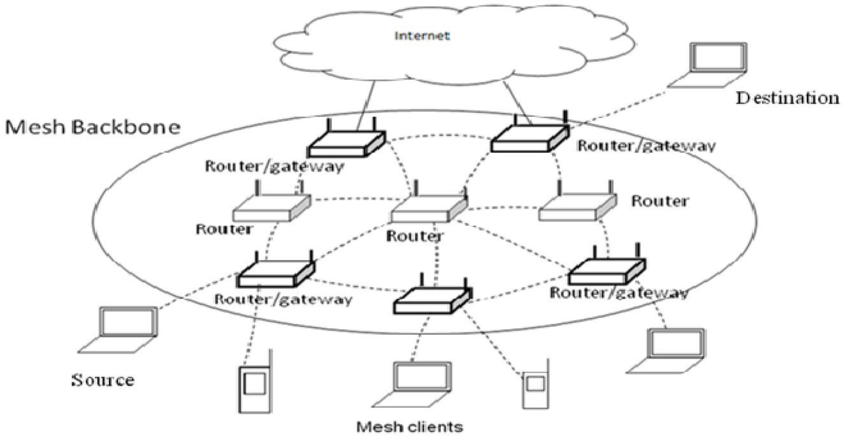

Figure 1.1 Infrastructure based WMNs

Client WMNs

These types of WMNs reflect an ad hoc network by providing peer to peer connectivity among the nodes in the network without using any infrastructure. Here, client nodes form the network by performing routing and other configuration functionalities in addition to the role of hosts. Hence, mesh routers are not required. In client WMNs, the communication among the nodes is done through multi hop forwarding. The network is formed by any one type of radios. Generally, mesh routers can be provided with multiple radios to perform routing and access functionalities. But in Client WMNs, one type of radio is used among the client nodes to perform routing and other configuration functionalities. Moreover, the complexity of client nodes is more compared to infrastructure based WMNs because the client nodes have to carry out additional functionalities such as routing and self configuration in addition to servicing users (Akyildiz et al. 2005).

Hybrid WMNs

It is the combination of infrastructure based WMN and client WMN. Mesh clients can be directly connected to other mesh clients or they can access the network through mesh routers. As in infrastructure based WMNs, backbone provides connectivity with other external networks and also to connect with the Internet. The routing functionality of mesh clients provides better network coverage in WMN (Akyildiz et al. 2005).

Characteristics of WMNs

WMN is defined as a wireless cooperative communication infrastructure among large number of wireless transceivers. The multi hop forwarding nature of WMN achieves the communication in a cooperative way. It supports ad hoc networking and also each node has the capability of self configuring, self healing and self organization. Hence, WMN provides more benefits to the users such as low deployment cost, ease of maintenance and better scalability (Redwan & Kim 2008, Akyildiz et al. 2005). By having radio nodes as mesh routers, WMN provides move coverage area compared to other wireless networks without sacrificing channel capacity. WMNs are more reliable since each node is connected to several other nodes. If one node drops out of the network due to hardware failure or some other reason, its neighbor nodes merely find another route. WMNs comprise two types of nodes such as mesh routers and mesh clients (Nandiraju et al. 2007). Mesh routers are static and power enabled while mesh clients are stationary or mobile nodes. WMNs support peer to peer communications as well as communications with the Internet (Akyildiz et al. 2005). WMNs are more compatible and also have better interoperability with the other wireless networks. When number of devices in WMN is high then the network offers more bandwidth which is the major requirement to support real world applications.

Advantages of WMNs

Due to the availability of wireless infrastructure or backbone in the network, WMN provides more coverage area, good connectivity and robustness during link failures. The conventional client nodes can use same radio technology as the mesh router nodes. WMN supports integrating with other wireless networks such as WI-Fi, Wi-Max, Internet, cellular and sensor networks through gateway nodes available in the mesh backbone. By having mesh routers in the backbone, WMN provides dedicated routing and configuration functionalities. Mesh routers are equipped with multiple radios to perform routing and access functionalities.

Application Scenarios of WMNs

Few applications of WMNs are listed as follows (Akyildiz et al. 2005):

- Broadband home networking
- Community and neighborhood networking
- Enterprise Networking
- Metropolitan Area Networking
- Transportation Systems
- Security and Surveillance Systems
- Health and Medical Systems

1.3 ROUTING PROTOCOLS IN WIRELESS NETWORKS

Routing is the process of discovering the end to end path from source node to destination node. Routing protocols are the heart of multi-hop wireless networks as they control the creation, configuration and maintenance of the topology of the network (Siva Nageswara Rao et al. 2011). Based on routing strategy used, routing protocols in wireless networks can be classified as proactive, reactive and hybrid (hierarchical) routing protocols. Since WMNs share the common features with ad hoc networks, the routing protocols designed for ad hoc networks can be incorporated in WMNs with necessary modifications.

1.3.1 Proactive Routing Protocols

Here, the routing paths are discovered regardless of the readiness of a node to transmit data. Routing tables are maintained at each node and the discovered routes are stored in the tables. Whenever a node wants to transmit data, it refers to the routing table. If the required path is available, it utilizes the path information to transmit data. Otherwise it initiates the route discovery process. Periodically, the routing information is exchanged among the nodes and stored in the routing tables at each node. Hence, these protocols suffer from high amount of control packets overhead and more power consumption even there exists no data transmission in the network. Optimized Link State Routing (OLSR) and Destination Sequenced Distance Vector (DSDV) routing protocols are the most popularly used proactive routing protocols.

Optimized Link State Routing (Clausen & Jacquet 2003) is an optimized version of link state algorithm designed for ad hoc network. It is a proactive routing protocol and thus routes are always available in the routing table (Ishfaq 2014). The aim is to minimize duplicate retransmissions in the same area. All nodes in the network exchange routing information periodically to maintain topology updates. Multipoint Relay (MPR) selectors are unique to OLSR so that nodes selected as MPRs only forwards control packets thereby reduces control overhead substantially. Each node broadcasts hello packets periodically to search next hop neighbours, MPR selection process and also for link sensing. Every node can get topology information up to two hops from the hello packets and thus used for calculating MPR set. Every node maintains MPR selector table where nodes selected as MPRs are recorded and updated periodically. Hence, each node broadcasts only its MPR selector information rather than broadcasting the whole neighbour information. Intermediate nodes, by receiving the MPR information, recalculate and update the routes to the known destinations.

Destination Sequenced Distance Vector Routing Protocol (Perkins & Bhagwat 1994) is a proactive routing protocol which is designed based on the traditional Bellman Ford algorithm. Sequence numbers are used in DSDV routing protocol to avoid formation of routing loops. At every node, routing table is maintained which stores next hop information towards a destination, cost metric for a path to the destination node and a destination sequence number. Periodically, each node transmits the updated routing information to its neighbour nodes. In this protocol, the route with highest sequence number is selected for packet transmission (Liu et al. 2008).

1.3.2 Reactive Routing Protocols

These are also known as on-demand routing protocols where route discovery process is initiated whenever a node wants to transmit data to some other node. Even though, the overhead caused by the control packets occur only on demand, it requires additional latency for route discovery before the data are delivered. In these schemes, nodes maintain routes to active destinations in their routing tables. For unknown destination node, a new route discovery process should be initiated. Ad hoc On-Demand Distance Vector (AODV) routing protocol and Dynamic Source Routing (DSR) protocol are two commonly used reactive routing protocols designed for ad hoc networks (Ishfaq 2014). AOMDV (Ad-hoc On-Demand Multipath Distance Vector) (Marina & Das 2001) is another on demand multipath reactive routing protocol. It provides better fault tolerance by discovering multiple link disjoint and loop free paths from source to destination.

Dynamic Source Routing (David et al. 2007) is a popular reactive source routing protocol where route discovery and maintenance processes are initiated on demand and source routing algorithm is implemented. In DSR, each data packet contains complete routing information to reach the destination. The major phases in DSR are route discovery and route maintenance. During route discovery, each node broadcasts a Route Request (RREQ) packet along with its source routing table. Upon receiving the RREQ message, each intermediate node appends its own identifier to the routing table in the routing message and forwards to its neighbour nodes. For every intermediate node, it is repeated until it reaches the destination and then destination unicasts Route Reply (RREP) packet to the source node. DSR incurs additional overhead since data packets carry the entire routing information during the hop by hop transmission which degrades the network performance (Liu et al. 2008).

Ad hoc On demand Distance Vector (AODV) (Perkins & Royer 1999) is another familiar reactive on demand routing protocol designed for mobile ad hoc networks which is based on both DSDV and DSR. Hence, it owns the advantages of both protocols like keeping track of destination sequence number to avoid routing loops etc. Contrast to these two protocols, in AODV, each node has to maintain only the routing information about the source, destination and next hop information which in turn minimizes the traffic overhead. Route discovery process in AODV is designed as same as DSR by broadcasting RREQ control packets. An intermediate node or the destination node unicasts RREP control packet when active route is found (Liu et al. 2008).

1.3.3 Hybrid Routing Protocols

Hybrid routing protocols are the combination of table driven and reactive routing protocols and thus take advantages of best features of both types. The aim is to reduce the control overhead occurring in proactive routing approaches and to minimize the delay caused for reactive route discovery approaches. Nodes which are available within the particular geographical area in the network belong to a common routing zone and proactive routing protocol is used in that zone. For nodes which are located outside the zone, route discovery is performed in a reactive way. Hence in hybrid routing protocols, route discovery takes place by using both proactive and reactive routing approaches. These protocols are also classified based on zonal and convergence characteristics. Zonal Routing Protocol (ZRP) is the hybrid routing protocol designed for ad hoc networks where both proactive and reactive routing protocols are implemented at different network areas. In convergence approaches, on demand mechanisms are needed to change the protocol functionality from proactive to reactive or vice versa. ChaMeLeon (CML) (Ramrekha & Politis 2010) is an adaptive hybrid routing protocol designed based on convergence approach. Convergence approach does not maintain routing zones.

Zonal Routing Protocol is a hybrid wireless networking protocol proposed by Haas et al. (2002) to speed up the packet delivery process and to minimize the control overhead by making use of both proactive and reactive routing approaches. For each node in the ad hoc network, a routing zone is defined separately. Nodes which are within the same routing zone can use proactive routing approach. For nodes outside the zone, route discovery is initiated by using an on demand approach. ZRP uses two sub routing protocols namely Intra-zone Routing Protocol (IARP) which is proactive and is used within the routing zone. The other one is Inter-zone Routing Protocol (IERP) which is reactive and is used between the routing zones (Kaur et al. 2013, SreeRangaRaju & Mungara 2011).

In this thesis work, we have proposed the routing protocols which are designed based on reactive routing approach. Route discovery process is carried out on demand by any node (source) by broadcasting Route Request (RREQ) packets and destination node unicasts a Route Reply (RREP) packet to the source node. The routing fields in RREQ and RREP packet are modified according to the security and performance enhancements made in the proposed approach. Destination node receives RREQ packets through multiple routing paths and it selects an optimal routing path through which RREP packet is unicasted.

1.4 ROUTING CHALLENGES IN WMNs

1.4.1 Security Issues in WMNs

Security issues for WMNs are basically identical to security requirements needed for any wireless communication system (Sgora et al. 2013, Redwan & Kim 2008). They are listed as follows: Availability, Authenticity, Integrity, Confidentiality and Non repudiation. Availability ensures the survivability of network services regardless of Denial of Service (DoS) attacks. This requirement is more challengeable during the DoS attacks since any node in the network can be the attack target and thus some selfish nodes make some of the network services unavailable (Gao et al. 2010). Authenticity assures the identity of participating entities in the network. Without the authenticity property, an adversary could ensure the identity of a communicating node. In the absence of authenticity, an adversary could impersonate a node and thus gaining unauthorized access to confidential resources, sensitive information and also interfering with the operation of other nodes (Eissa et al. 2013).

Integrity property guarantees that a message being transmitted in the network cannot be modified by intruders (or unauthorized users). Integrity can be compromised in two ways. One is due to malicious altering (e.g., an attacker alters the account number in a bank transaction intentionally) or due to transmission error (e.g., the amount to be withdrawn is transmitted incorrectly) (Siddiqui & Hong 2007, Zhang et al. 2006). Confidentiality guarantees that certain information is only accessible to those who have been authorized to access it. In other words, certain information should not be disclosed to unauthorized entities. Non-repudiation property ensures that both the sender and the receiver of a message communication cannot deny that they have ever sent or received such a message (Sgora et al. 2013).

1.4.2 Privacy Issues in WMNs

The basic privacy issues for WMNs are identified as follows: Authorization, Anonymity, Access Control and Accountability. Authorization is a process in which an entity is provided with credentials by means of the trusted certification authority. It is generally used to assign different access rights to different level of users (Malik et al. 2011). Anonymity means that all the information that can be used to identify the communicating entities should be kept private and not distributed to other unauthorized entities (Sgora et al. 2013, Redwan & Kim 2008). Access Control property guarantees that only authorized actions can be performed in the network (Zhang & Fang 2006, Hu & Perrig 2004). And also, access control involves the authentication and authorization of the network entities of the WMNs (Egners & Meyer 2010). Accountability property aims to detect misbehaving entities and, if it is necessary, in many cases to deny network access to them via revoking, so that malicious users can be avoided (Ren et al. 2010).

1.4.3 Factors Influencing Optimal Routing

The features required to design an optimal routing are identical to the factors influencing network performance which are as follows: Performance Metrics, Scalability, Robustness, Fault tolerance, Adaptive support of Mesh Routers and Mesh Clients, Cross layer Interaction, Broadband and Quality of Service (QoS) (Akyildiz et al. 2005). With respect to performance metrics, new metrics have to be discovered and utilized to enhance the performance of routing protocols. Routing set up in a large network is time consuming. Node states on the path may change rapidly. Hence, scalability of routing protocols is critical in WMNs. To provide better performance, WMNs must be robust against link failures or congestion and can achieve load balancing. Mesh routers have minimal mobility and there is no constraint on power consumption, energy, etc. whereas mesh clients are mobile and have power, energy constraints. Hence, design of efficient routing protocols for WMNs by adaptively supporting both mesh clients and mesh routers is more important. Cross layer interaction must be needed during route discovery to improve the network performance of the routing protocol. Compared to other ad hoc networks, WMNs are in need of broadband services with various QoS requirements. Hence, in addition to end-to-end delay and fairness, some more performance metrics such as bandwidth, delay jitter and packet loss ratios have to be considered in routing protocols.

In this thesis work, we are focusing on addressing security issues, privacy issues and also few performance issues in infrastructure based WMNs by proposing optimal privacy preserved and secure routing approach for WMNs.

1.5 SECURITY ATTACKS IN WMNs

The protocols applied for different layers of communication stack of WMN have more security vulnerabilities due to the potential attacks at various layers. Hence, network services are disrupted and in turn network performance is highly degraded. The existing protocols are designed by the assumption that the nodes are honest and cooperate well during forwarding of packets. However, few nodes may become malicious or compromised by the selfish nodes (Sen 2013). Depending on whether the network functionality is disrupted or not, the attacks can be classified into passive attacks and active attacks (Pervaiz et al. 2010). The main aim of an active attacker is to disrupt the network operation, where as a passive attacker wants to eavesdrop or steal the information during data communication within the network (Sgora et al. 2013, Santhanam et al. 2008).

Passive attacks would negate confidentiality while active attacks lead to the violation of security requirements such as availability, authentication, integrity and non-repudiation. Active attacks can be further classified into internal (or insider) and external (or outsider) attacks. External attacks are carried out by the outsider nodes by eavesdropping the communication or injecting false information into the network. Internal attacks are performed by the participant nodes of the WMN to conduct severe malicious actions which are very difficult to detect than the external attacks (Sgora et al. 2013, Santhanam et al. 2008).

1.5.1 Security Attacks in Physical Layer

Since the mesh routers of WMN can be placed in roofs of buildings or on street lamps, the physical protection of mesh routers is very weak. They can be easily tampered and also sensitive information may be extracted from them. In addition to that, physical layer can also be affected by jamming attack which interferes with the radio frequencies of the nodes used in the network for communication (Lazos et al. 2011, Glass et al. 2008). Three types of jamming attacks are normally exploited at physical layer as described in (Seth & Gankotiya 2010).

- The trivial jamming attack: An attacker transmits noise constantly.

- The periodic jamming (or scrambling) attack: An attacker sends out a short signal at regular intervals.

- The reactive jamming attack: An attacker intentionally sends out a signal whenever it identifies that another node has initiated a transmission.

1.5.2 Security Attacks in Link Layer

Link layer of WMN undergoes different type of attacks. Some of the attacks at this layer are: passive eavesdropping, jamming attack, Medium Access Control (MAC) address spoofing attack, flooding attack etc. Passive eavesdropping attack can be launched by external as well as internal attacker nodes. Due to the broadcast nature of transmission in wireless networks, these networks are very much prone to passive eavesdropping attack by the external attackers which are within the transmission range of the nodes. WMNs are also prone to internal eavesdropping attacks by the intermediate hops, whereby a malicious intermediate node may contain the copy of all the data which it forwards without the knowledge of the related nodes in the network (Sen 2011). Even though passive eavesdropping attack does not affect the network functionality directly, it leads to the compromise in confidentiality and integrity of data. To ensure these properties, encryption with strong keys is generally incorporated during data communication. Link layer jamming attacks are more complex compared to physical layer jamming attacks (Lazos et al. 2011). In this case, an attacker node transmits regular MAC headers on the transmission channel instead of transmitting random bits constantly. MAC address spoofing attack can be launched during the transmission of MAC frames where an attacker tries to modify the MAC address in the frames (Naveed et al. 2009). Flooding attack is launched by an attacker node by sending a lot of MAC control messages to its neighbour nodes. Hence, the fairness of medium access is physically abused (Sen 2011).

1.5.3 Security Attacks in Network Layer

The attacks occurring at network layer of WMN can be divided into two types: control plane attacks and data plane attacks. Control plane attacks target the routing functionality of the network, while data plane attacks affect the packet forwarding functionality of the network.

Control Plane Attacks

Few of the control plane attacks are listed as follows: Rushing attacks, Routing table overflow attack, Sybil attack, Byzantine attack, Wormhole attack, Sinkhole (or black hole) attack, Gray hole attack, Sleep deprivation attack, Location disclosure attack, Route error injection attack, etc. Rushing attacks target the on demand routing protocols like AODV, DSR, etc. The attacker aims to send a lot of route request control packets continuously across the network within a short interval of time to cause the other nodes busy with processing legal route request packets. Routing table overflow attack caused by an attacker node which attempts to create routes to nonexistent nodes with the intention of preventing new routes from being created by overwhelming the routing tables and also disrupts the route discovery process (Divya & Kumar 2010). Sybil attack can be launched by an attacker node which attempts to create multiple identities in the network, each appearing as a legitimate node with the intention of disrupting the normal functionality of the network (Naveed et al. 2009, Redwan & Kim 2008). Byzantine attack is launched by a single malicious node or by a group of compromised nodes to create routing loops and attempts to forward packets in long routes instead of optimal routes or may drop packets. Successful launching of this attack degrades network performance and also disrupts the network services.

Wormhole Attack is another severe attack leads to Denial of Service (DoS) where an attacker node records packets at one location in the network, tunnels them to another compromised node through a wormhole or through a private network, and retransmits them from there into the network (Naveed et al. 2009, Hu & Perrig 2004). Sinkhole (or black hole) attack can be launched by an attacker node which always replies positively to a RREQ packet coming from the neighbours, even though it may not have a valid route to the destination. The malicious node simply drops the received packets. Gray hole attack is a variant of black hole attack. In the case of black hole attack, attacker or malicious node drops all the packets that it is supposed to forward which may lead to possible detection of the attack. On the other hand, in a gray hole attack, the attacker drops the packets selectively and makes the attack detection as difficult. A gray hole attack does not lead to complete denial of service, but it may go undetected for a long period of time (Sen 2013, Seth & Gankotiya 2010). Sleep deprivation attack occurs when a malicious node attempts to drain the batteries of a victim node by forwarding route request packets, or by sending unnecessary packets to it. Location disclosure attack can be created by adversary node which attempts to disclose the information about the location of nodes or about the network topology information to the intruders or attackers (Wu et al. 2007). Route error injection attack can be caused by a malicious node which injects forged route error packets to break the links and disrupt the routing services.

Data plane attacks

These types of attacks are launched by selfish and malicious nodes within the network and cause performance degradation or denial of service attack. The simplest of data plane attack is passive eavesdropping. It is a kind of MAC layer attack. Selfish behaviour of the participating WMN nodes is a major security issue since the WMN nodes are dependent on each other for data forwarding (Chong et al. 2013). It is hard to distinguish between such a selfish behaviour and the link failure or network congestion. Considerable network resources such as bandwidth, CPU cycles for packet processing, etc are consumed to forward the junk packets which may lead to denial of service for valid user traffic. The attacker nodes may also inject the maliciously crafted control packets which may lead to the disruption of routing functionality (Sen 2013).

In this thesis work, we are focusing on the detection of security attacks at network layer in WMN. Generally, the internal malicious nodes are more difficult to detect in wireless networks than the external attacker nodes. Thus, we have proposed efficient security mechanisms for WMNs to defend against severe internal packet dropping and misdirecting attacks such as worm hole, black hole, gray hole and also other network layer attacks like misrouting and power control attacks, Sybil attack, hello flood attacks and route disruption attacks.

1.6 DEFENSE MECHANISMS

WMNs are more vulnerable to attacks due to the built in features such as dynamic topology, absence of centralized administrator and open shared medium of communication. Hence, efficient defense mechanisms are required to defend against malicious attacks.

1.6.1 Secure Routing based on Cryptographic Mechanisms

To provide availability in WMNs, routing protocols should be robust against both dynamic topology and malicious attacks. In literature, several routing protocols for WMNs have been proposed (Seth & Gankotiya 2010). However, these protocols have strong assumption that intermediate nodes would cooperate well during forwarding of packets. But, this may not be always true in WMNs. There exist several security threats (Redwan & Kim 2008), some occurring from weakness in the routing protocols, and others from the absence of conventional identification and authentication mechanisms (Siddiqui & Hong 2007).

There are two types of threats targeting the routing protocols. The first one is external attack. By injecting false routing information, replaying old routing information, altering the routing information, an attacker could successfully launch an attack or introducing excessive traffic load into the network. The second kind of threat which is more severe to detect come from compromised internal nodes which might advertise incorrect routing information to other nodes. Detection of such incorrect information is difficult since merely requiring routing information to be signed by each node would not work, since compromised nodes are able to generate valid signatures using their private keys.

To protect against the first kind of threats, strong encryption and efficient authentication mechanisms are required. However, this defense mechanism is ineffective against attacks from internal compromised adversary nodes. On the other hand, incorporating route redundancy (e.g., protocols such as Zonal Routing Protocol (ZRP), Dynamic Source Routing (DSR), Ad hoc On demand Multipath Distance Vector (AOMDV) and Temporally Ordered Routing Algorithm (TORA)) during route discovery can be implemented for secure routing. If the current routing path is failed, nodes can use an alternative route. Multipath routing (Sen 2011) provides the benefit of using multiple routes in an efficient way without message retransmission. The basic idea is to broadcast redundant information through additional routes for error detection and correction. To address the security attacks at routing layer, several secure routing protocols have been proposed in the literature such as Secure Ad Hoc On-Demand Distance Vector (SAODV), Ariadne, Secure Efficient Ad Hoc Distance Vector (SEAD), Secure Routing Protocol (SRP) and Authenticated Routing for Ad Hoc Networks (ARAN) based on public key cryptographic mechanisms (Siddiqui & Hong 2007). However, relying on public key cryptosystems alone does not provide complete security against the internal attacks. In this thesis work, we have applied Elliptic Curve Cryptographic (ECC) algorithms for signature, key exchange, encryption and decryption processes in the proposed mechanisms. ECC mechanism has more advantages such as more security strength, faster and better performance compared to other cryptographic schemes (Jeong et al. 2006).

1.6.2 Intrusion Detection Mechanisms

Due to the characteristics of WMNs such as an open shared medium, dynamic topology, and the absence of centralized administrator, the intrusion detection techniques which are developed for a fixed wired network are not suitable for WMNs. Zhang et al. (2003) have proposed a detailed design of intrusion detection and response mechanisms. Marti et al. (2000) have proposed two Intrusion Detection System (IDS) mechanisms: watchdog and pathrater, which enhances throughput in the presence of selfish nodes also. The IDS monitors and collects the activity information from all the nodes and then analyzes it to determine whether there are any malicious activity is present or not. Once the IDS detects that there is an unusual activity, an alarm is generated to alert the security administrator. Besides, IDS can also start a proper response to the malicious activity. Based on the architectural design, IDS can be classified as follows (Siddiqui & Hong 2007): (i) Stand-alone Intrusion Detection Systems which runs on each node independently to detect intrusions. (ii) Distributed and Cooperative Intrusion Detection Systems (Zhang et al. 2003), in which an IDS agent runs on each node and nodes participate in intrusion detection and response. An IDS agent takes the responsibility of detecting and collecting local events and data to identify possible intrusions and also initiating a response independently and (iii) Hierarchical Intrusion Detection Systems in which nodes form clusters and cluster heads act as control center to provide the functionality for its child nodes. It is very difficult to install IDS on each mobile client node in WMN and thus distributed IDS and hierarchical IDS are suitable for WMNs. This thesis work does not focus on IDS.

1.6.3 Reputation and Trust Mechanisms

Reputation and trust are two popular and useful tools that are used to facilitate decision making in wireless communication scenarios. Reputation is defined as the opinion of one entity about another. In effect it signifies the trustworthiness of an entity. On the other hand, trust is defined as the expectation of one entity about the actions of another entity (Sen 2006). The essential objectives of reputation and trust-based systems for wireless communication networks have been discussed in (Siddiqui & Hong 2007, Sen 2006). They are as follows: (i) providing information that allows nodes to distinguish between trustworthy and untrustworthy nodes in the network, (ii) encouraging the nodes in the network to cooperate with each other and become trustworthy, (iii) discouraging the untrustworthy nodes to participate in the network activities. Two additional goals of a reputation and trust-based system in wireless communication systems are identified by Sen (2006). The first one is to increase the viability of the system in any kind of visible malicious activity, and the second is to minimize the damages caused by any insider attacks.

Trust and security are the two mutually dependant concepts which cannot be separated (Siddiqui & Hong 2007). For instance, trust cannot be ensured without the analysis of secure communication, likewise security attributes such as cryptography requires trusted key exchange mechanisms (Eissa et al. 2013). WMN communications are based on “trusting the neighbors” relationships. As the WMN environment is assumed as cooperative, these trust relationships are very much prone to attacks. Moreover, the inherent features of WMN such as the lack of fixed trust infrastructure, resource limitations, temporary connectivity and availability, open shared wireless medium and physical vulnerability, make trust establishment almost impossible. Hence, the distinct properties of trust management in WMN are: uncertainty and incompleteness of trust evidence, neighborhood trust information exchange and distributed computation. Hence, the trust evaluation is performed in a highly decentralized way.

To overcome these problems and to establish trust in WMN, some assumptions are incorporated including pre-configuration of nodes with secret keys, or existence of a central trust authority. Direct trust between two communicating parties can be established using the authentication mechanisms. Third party trust is employed by keeping a trusted certificate authority. In literature, various trust computation and reputation mechanisms have been proposed based on interactions with one-hop neighbors (Siddiqui & Hong 2007) (Ferraz et al. 2014).

To enforce security against malicious nodes, several reputation mechanisms have been proposed in the existing systems. The major objectives of these systems are to monitor the behavior of the neighbor nodes and also to evaluate the reputation metrics of the neighbor nodes. However, these mechanisms are not sufficient to provide complete privacy protection and better link reliability in WMN. The communication in WMNs has different kinds of sensitive user information in different situations which have to be protected and secured from the unauthorized nodes like malicious nodes. Hence, strong privacy protection and secure routing mechanisms are required to protect communication that involves sensitive information in WMNs.

In this thesis work, we have incorporated a reputation mechanism named extended local monitoring technique to detect and isolate two severe packet dropping attacks such as misrouting attack, power control attack. We have also proposed a new Cross-Layer and Subject Logic based Dynamic Reputation (CLSL-DR) mechanism to protect the network against packet dropping and misdirecting attacks.

1.6.4 Key Management Mechanisms

These mechanisms require a key management server which takes the responsibility of keeping track of bindings between keys and nodes and also for aiding establishment of secure communication and mutual trust between nodes. In the traditional cryptographic mechanism, a session key is generated at one end and it is encrypted by the public-key encryption algorithm. Then it is delivered and recovered at the other end. In the symmetric security approach, a sequence number or a nonce could be included to thwart the replay attack while setting up a session key (Kandah et al. 2011). There are three categories of key management approaches that can be applied on WMNs (Wu et al. 2007): the first one is virtual Certificate Authority (CA) approach, the second one is certificate chaining approach, and the third one is composite key management approach, which combines the first two.

In this thesis work, we have applied composite key management approach to implement the proposed mechanisms. In one mechanism, it is implemented as follows: In offline, each new node has to register with the CA by sending its personal details and in turn, it gets information about key generation mechanisms from CA. These nodes generate their public and secret keys accordingly and forward their public key to CA. We have applied anonymous key generation algorithm in another mechanism in which an offline key server is kept which generates group public key (gpk) and group signature key (gsk) for each registered user in the network. The key server also generates a master secret key and an ID based key for every node in the network. By having these keys, each node establishes a session key with each neighbour node within its radio range for effective route discovery and data communication. This key establishment process is employed based on an efficient security scheme such as Elliptic Curve Diffie Hellman (ECDH) key exchange.

Thus, we have designed privacy preserved secure routing approach based on cryptography and trust management mechanisms. This approach is able to provide better security and privacy protection in WMNs. Moreover this approach is able to deal with both internal and external attacks.

1.7 MAJOR CONTRIBUTION OF THE THESIS

In this thesis work, we are focusing on designing optimal privacy preserved and secure routing in WMNs by ensuring privacy preserving properties, security requirements and also by incorporating enhanced routing metrics during route discovery. We also focus on detecting packet dropping and misdirecting attacks occurring in network layer caused by selfish behavior of the adversary nodes and also some internal attacks such as Sybil attack, hello flooding attack, route disruption attacks etc. There exists high demand of supporting real-time multimedia applications over WMNs. Hence, QoS support is essential for WMNs. Thus we also focus on effective QoS provisioning for optimal routing in WMN by providing better reconfiguration plans and enhanced routing metrics. We propose three different approaches for optimal secure routing in WMNs.

The first approach is privacy preservation for optimal secure routing to provide complete privacy protection and to defend against packet dropping attacks in WMNs. Based on this approach, we have proposed two routing protocols namely Privacy Based Optimal Routing (PBOR) and Unobservable Privacy preserved Secure Routing for Mesh networks (UPSRM). Security card model is introduced in PBOR to provide hop by hop authentication and anonymity in routing. Besides the most commonly used routing metric such as hop count, the proposed scheme applies the enhanced routing metrics of Distrust Value (DV) and Bandwidth Aware Metric (BAM) in the process of route discovery. The above metrics are computed at each node and the route discovery process uses these metrics for selecting an optimal path among the many alternate paths that are available from source to destination. The selected optimal path is able to defend against packet dropping and misdirecting attacks. We have performed simulation and compared with the similar privacy preserved secure routing protocol in both malicious and non malicious environment. The results prove that the proposed scheme performs better in malicious environment with most of the parameters chosen for performance evaluation.

UPSRM protocol is proposed to provide stronger privacy preserved secure routing in infrastructure based WMNs by providing the features of anonymity, unobservability and unlinkability. The proposed technique incorporates group signature and ID based encryption schemes to achieve these properties. By reviewing the existing works, it has been found that the existing privacy preserved secure routing schemes do not deal with unobservability of packets in infrastructure based WMNs. Unobservability is required for content and pattern protection of packets that flow in the network in order to prevent attacker viewing the content of the packet and finding the type of the packet. The major advantage of UPSRM is that it provides anonymity and unlinkability to preserve privacy of nodes, and unobservability to provide security to packets that flows in the network. It protects the network against packet dropping and misdirecting attacks such as wormhole, black hole, gray hole and jellyfish attacks by using Neighbors Passive Acknowledgement Mechanism (NPAM). It also provides an optimal path for data transmission by computing bandwidth of the path using cross layer information exchange. The simulation results show that UPSRM provides better security and privacy protection compared to the existing mechanisms and the observed tradeoff in terms of delay due to the implementation of enhanced routing metrics.

The second approach is reputation maintenance for optimal secure routing to monitor the behavior of the neighbor nodes. Reputation maintenance is needed in WMNs to give the information which allows nodes to distinguish between trustworthy and untrustworthy nodes in the network and also to encourage the nodes in the network to cooperate with each other and become trustworthy. Here, we propose two protocols namely Secure Efficient Routing against Packet Dropping Attacks (SERPDA) and Trust based Secure Reliable Routing (TSRR) protocol. SERPDA is proposed to detect and isolate two severe packet dropping attacks such as misrouting attack and power control attack in WMN in which an extended local monitoring technique is implemented. Some MRs are designated as guard nodes that maintain additional next-hop information gathered during route discovery and also check the forwarding pattern of neighbors to defend against the packet dropping attacks. To address network performance, multiple routing metrics are integrated during route discovery to find out an optimal path. The simulation results show that SERPDA provides better performance compared to existing routing protocols AODV and SADEC by choosing the optimal path. The simulation results also show a slight increase in delay compared to SADEC due to the overhead caused by routing metrics enhancement.

TSRR is designed to propose a trust based secure routing algorithm for enhancing security and reliability of WMNs. TSRR employs a new Cross Layer and Subject Logic based Dynamic Reputation (CLSL-DR) scheme along with security tag model. This model uses only the trusted nodes with forwarding reliability for data transmission and it isolates the malicious nodes from the providing path. Moreover, every node in this model is assigned with a security tag which is used for efficient authentication. Incorporating CLSL-DR mechanism in route discovery provides better protection against packet dropping and misdirecting attacks. Thus, by combining authentication, trust and subject logic, the proposed approach is capable of choosing the trusted nodes effectively to participate in forwarding the packets of trustful peer nodes successfully. It also provides optimal path for data transmission by selecting only secured and reliable path during route discovery. The simulation results obtained from this work show that the proposed routing protocol provides optimal network performance in terms of security and packet delivery ratio.

The third approach is Effective QoS provisioning for optimal routing which provides better QoS aware reconfiguration plans to recover from frequent link failures in WMNs. There exists high demand of supporting real-time multimedia applications over WMNs. Hence, QoS support is essential for WMNs and we have proposed a protocol named Efficient Routing with QoS aware Reconfiguration (ER-QAR). Here we introduce hybrid routing metric during route discovery which establishes an efficient routing path by considering the link quality and performance parameters. By integrating self reconfiguration system with the routing protocol, QoS aware reconfiguration plans are determined. These QoS aware reconfiguration plans play a major role during link failures. Simulation results show that ER-QAR outperforms the traditional AODV in terms of the chosen parameters for performance evaluation. ER-QAR selects an optimal path by considering load balancing, link quality, transmission rate and number of hops and also effectively recovers the network from frequent link failures.

1.8 THESIS ORGANIZATION

The remainder of this thesis is organized as follows:

Chapter 2 provides a detailed literature review on wireless ad hoc networks, privacy preservation mechanisms, secure routing protocols and efficient routing protocols based on performance based routing metrics. The advantages and issues of the existing mechanisms are discussed.

Chapter 3 discusses privacy preservation approach for optimal secure routing in WMNs and under that two routing protocols are proposed based on security card model and anonymity based key generation model to provide strong privacy protection in WMNs. Also the protocols provide better network performance by enhancing the routing metrics. This chapter also presents the simulation results of the proposed protocols and comparison analysis with the existing routing protocols.

Chapter 4 explains an approach named reputation maintenance for optimal secure routing for WMNs and under that approach two routing protocols are proposed to defend against internal attacks effectively and to design high performance secure reliable routing path. This chapter also discusses the results of the simulation and detailed performance and security analysis of the two protocols in comparison with existing mechanisms.

Chapter 5 describes the effective QoS provisioning approach for next generation applications by providing better reconfiguration plans and to recover from local link failures. The simulation results are presented by analyzing the performance of the proposed protocols with similar existing routing mechanisms.

Finally, **Chapter 6** concludes the thesis work by presenting a summary of the proposed approaches for optimal secure routing and provides possible directions towards future research.