1. Introduction

Mobile Ad Hoc Networks (MANET) consist of fixed or mobile nodes which are connected wirelessly and without the support of any fixed infrastructure or central administration. If two nodes are within each other’s transmission range, then communication can be direct otherwise through intermediate nodes or relay network. Nodes are self-organized and can be deployed anywhere. Nodes are free to move anywhere, anytime and at different speed. In a high mobility environment, the random and continued movement of nodes leads to a highly dynamic topology. These networks are characterized by meagre capacity caused by the noise and interference inherent in wireless transmission and multi-path fading, limited battery power of mobile devices, limited capacity, asymmetric/unidirectional links, rapid deployment, flexibility, robustness and highly dynamic network topology are some of the salient features of MANET.

Infrastructure less MANET facilitates several applications like: Vehicular Ad Hoc Networks (VANETs), military battle fields, disaster recovery, household appliances, alert systems etc. using cooperation of mobile nodes. MANETs can support advanced application links in civil application for sport events, audio/video conferencing, telemetric applications, military applications for group formation and movement of soldiers, tanks etc., in national situations for national crises- earthquakes, fire, floods, energy and rescue operations etc. and integration with cellular systems. As discussed earlier, sensor-based ad hoc devices available to construct MANET have scarcity of resources. In resource constraint mobile devices achieving goals of high throughput, minimum delay, minimum setup time, minimum power consumption, minimum use of gates and constructing a secure environment seem to be challenging. Cooperative nodes can add flexibility, expandability, portability, ease to construct routes, dependability etc. All these features open the doors of insecurity among nodes. A node offer with power, energy, memory etc. like baits can make it to behave selfishly which can lead to insecure network. In order to make these networks secure, three cryptographic primitives must be taken into consideration: (i) confidentiality, (ii) authentication and (iii) key management. Low capacity devices demand lightweight cryptographic primitive implementation.

In this work: A secure and lightweight hierarchical MANET is constructed with integration of Radio Frequency Identification (RFID) and Sensor devices. This network is made secure with integration of
cryptography primitives and protocols. Further, network is lightweight because lightweight key management, primitives and protocols are integrated for increasing the performance. The following sections describe the contemporary challenges in MANET, work done for identifying the lightweight primitives and protocols, issues identifies from literature, objectives of work and summary of chapters.

2. Contemporary Challenging R&D problems in Mobile Ad Hoc Networks

Following are the major challenges in MANET:

a. Meagre Capacity / Bandwidth Scarcity
   Low capacity mobile sensor devices have limited memory and computing capacity and thus bandwidth availability is limited.

b. Limited Battery
   Power consumption is another important challenge. Mobile devices have limited battery storage capacity and thus need regular recharge after certain period of time. Some centralized and decentralized mechanisms need to be integrated in order to achieve good quality service.

c. Robustness and highly dynamic network topology
   Ad Hoc and mobile nature of sensor based devices in MANET increases the chance to frequently construct or destruct the routing tables. Quick table updating means more energy requirement and more number of packet communications. This increases the overhead over network.

d. Security
   Security is a major concern. Limited capacity devices have limited reserved resources for security primitives. Any foolproof system demands five characteristics: (i) availability, (ii) confidentiality, (iii) authentication & authorization, (iv) key management and (v) non-repudiation. All these security primitives need to be implemented within limited software and hardware resources. Thus, there is need of ultralight features to be integrated in implementation of security primitives.

e. Design and implementation of routing protocols.
   Three major categories of routing protocols proposed for MANET are: proactive, reactive and hybrid. Enhancements to these protocols are still under research. New lighter mechanism for resource constrained devices with maximum throughput and efficient computing are major challenges.

f. Multi-path fading
   Signal fading due to physical obstacles, environment conditions, malfunctioning of sensor devices, interferences, masquerading etc. are other major challenges in this area.
3. Brief Literature Survey

RFID and Wireless Mobile Sensor Networks (WSNs) are the two prominent wireless technologies used to implement a complete smart environment. The integration of RFID with wireless mobile sensor node constructs MANET. This integration of mobile sensor nodes with RFID tags maximizes their effectiveness by extending the capabilities, scalability, cost reduction etc. Table 1 shows various single hop hierarchical MANETs. All single-hop hierarchical MANET concentrates on routing security aspects rather than network security. Similarly, Table 2 shows the anomaly detection based hierarchical MANET and all these systems also concentrate on routing security rather than network security aspects. Further, MANET is resource constrained network and require lightweight security solutions.

<table>
<thead>
<tr>
<th>Clustering Scheme</th>
<th>Performance Overhead</th>
<th>Network Security</th>
<th>Sub-group Stability</th>
<th>Number of sub-groups</th>
<th>Formation Technique</th>
<th>Radius</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCA, 2000 [3]</td>
<td>Lower</td>
<td>No</td>
<td>Highest</td>
<td>Lower</td>
<td>Weight</td>
<td>Single Hop</td>
</tr>
<tr>
<td>Bdelhak, 2013 [9]</td>
<td>Lower</td>
<td>No</td>
<td>Highest</td>
<td>Lower</td>
<td>Weight</td>
<td>Single Hop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Author</th>
<th>Network Security</th>
<th>Routing Attacks</th>
<th>Protocol</th>
<th>Technique</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albers et. al. 2002 [10]</td>
<td>No</td>
<td>No</td>
<td>Undefined</td>
<td>Anomaly</td>
<td>Simulation</td>
</tr>
<tr>
<td>Zhang et. al., 2003 [11]</td>
<td>No</td>
<td>Yes (Eclipse)</td>
<td>AODV, DSR, DSDV</td>
<td>Anomaly</td>
<td>Simulation</td>
</tr>
<tr>
<td>Sun et. al., 2003 [13]</td>
<td>No</td>
<td>Yes (Sybil)</td>
<td>DSR</td>
<td>Anomaly</td>
<td>Simulation</td>
</tr>
<tr>
<td>Sterne et. al. 2005 [14]</td>
<td>No</td>
<td>No</td>
<td>Undefined</td>
<td>Anomaly</td>
<td>Simulation</td>
</tr>
<tr>
<td>Lauf et. al. , 2010 [16]</td>
<td>No</td>
<td>Yes (spoofing, misleading etc.)</td>
<td>Undefined</td>
<td>Anomaly</td>
<td>Simulation</td>
</tr>
<tr>
<td>Joseph et. al., 2011 [17]</td>
<td>No</td>
<td>Yes (Sinkhole)</td>
<td>OLSR</td>
<td>Anomaly</td>
<td>Simulation</td>
</tr>
<tr>
<td>Kabiri et. al., 2011 [18]</td>
<td>No</td>
<td>Yes (DoS)</td>
<td>DSR, AODV</td>
<td>Anomaly</td>
<td>Simulation</td>
</tr>
<tr>
<td>Jabbehdari et. al., 2012 [19]</td>
<td>No</td>
<td>Yes (DoS)</td>
<td>Undefined</td>
<td>Anomaly</td>
<td>Simulation</td>
</tr>
<tr>
<td>Nadeema et. al., 2014 [20]</td>
<td>No</td>
<td>Yes (Black &amp; Gray hole, rushing etc.)</td>
<td>AODV</td>
<td>Anomaly</td>
<td>Simulation</td>
</tr>
<tr>
<td>Basabaa et. al., 2014 [21]</td>
<td>No</td>
<td>Yes (Collusions and collisions)</td>
<td>Undefined</td>
<td>Anomaly</td>
<td>Simulation</td>
</tr>
</tbody>
</table>
Lightweight Cryptography: Lightweight cryptography can be classified into primitives and protocols. The goal of lightweight primitives is to achieve confidentiality, integrity, authentication, availability, and non-repudiation [22]. Lightweight primitives can be classified as symmetric or asymmetric. Lightweight protocols can be classified as: identification, authentication, distance bounding, grouping proof, and tag ownership transfer protocols.

a. Identification Protocols: In code-based identification systems, the McEliece-based cryptosystem [23] is the first public-key linear error correcting codes (ECC) – based cryptosystem using Goppa codes, and is NP complete. This scheme has fast encryption and decryption functions and is efficient for resource-constrained embedded devices [24]. The major problem of this scheme is its large key size [25]. Various schemes [25]-[28] have been proposed to reduce the key size using different coding techniques. The Sidelnikov system with Reed-Muller codes [26] is an example of a reduced key length code–based cryptosystem. However, this system is prone to structural attacks [29]. Berger et. al. [25] proposed a reduced key generation process using Reed-Solomon codes in quasi-cyclic form. This coding mechanism is selected in this work for generating random codes and assigning identification marks for the current work because quasi-cyclic form of Reed-Solomon codes is having short and simple codes for keys, lesser encoding complexity (O(n)), no need to store any matrix value (e.g. generator or circulant matrices) and easy to implement.

b. Authentication Protocols: Sastry et. al. [30] proposed authentication through location verification. This time-based location verification approach requires extra hardware to verify locations. Capkun et. al. [31] proposed an on-the-spot verification algorithm that requires extra hardware. A representative hardware reduction technique has been proposed in [32]. This technique is affected with basic logic malfunctioning attacks [33]. In 2012, Tian et. al. [34] proposed a permutation-based authentication protocol to avoid attacks due to unbalanced OR and AND operations by using permutations. Permutation-based protocols are prone to de-synchronization, traceability, and disclosure attacks. However, attempts have been made to modify RFID authentication protocols with permutation (RAPP) to avoid de-synchronization attacks [33].

c. Grouping Protocols: In 2004, Juels was the first to propose the idea of generating evidence for the presence of a group of nodes [35]. Juels’ idea of grouping is for un-trusted users and was proposed to provide verifiable proofs [35][36]. Lamport extended this idea into two
mechanisms: basic construction and one based on Lamport digital signature construction [36]. However, this idea of grouping is prone to replay attacks, denial of service, and impersonation attacks. Recently, another lightweight authentication protocol that takes into consideration anonymity, authentication, and un-traceability was designed by Chein [37]. This system is based on ECCs and a public key–based Rabin cryptosystem.

**Attacks:** Dynamic topology, an open medium, distributed nodes, fluctuating link capacity, limited energy, scarcity of resources, and so on make a system vulnerable to attacks. External and internal attackers impersonate the identities and privileges of other nodes so as to disturb a network. Sybil [38][39], eclipse [40], and de-synchronization [41][42] are examples of such control traffic attacks and are described as follows:

- **Sybil attack** [38][39]. In this type of attack, a malicious node behaves as a legitimate node by impersonating or stealing the identity of a node. The methods to limit this attack can be classified as: (i) Strong identification of peers [38], (ii) Authentication and authorization and (iii) Trust score [39]

- **Eclipse attack.** In a network, many versions of this attack are possible. This attack does not directly disrupt the network but it boosts other attacks. In this attack, an attacker tries to capture neighboring nodes that can be easily compromised. Malicious nodes conspire to mislead correct nodes to control traffic. This enables flooding, denial of service, or censorship attacks. Mechanisms to defend against this kind of attack are classified as [40]: (i) Structural constraints and (ii) Proximity constraints

- **De-synchronization attack.** An attacker can break the synchronization between RFID reader and RFID tag to use different identity pseudonyms. Different identity pseudonyms between RFID reader and RFID tag result in a de-synchronization attack [41]. In [42], a de-synchronization attack is analyzed over a hash-based mutual authentication scheme. This work states that a de-synchronization attack can be avoided by adding additional messages to acknowledge the identity pseudonyms. However, Deursen et. al. [43] analyzed that sending an acknowledge packet does not prevent such an attack.

**Other Security Challenges**

MANET is a pervasive system. Security of this system is equally important. An attacker can object to harm the system at various points. These points include information eavesdropping during...
transmission or storage, obstructing physical access to devices, capturing the devices and stealing the information etc. Protection from these threats demands strong mechanism for confidentiality, integrity, authentication, availability and non-repudiation. This protection mechanism should addresses major security concerns in RFID mobile sensor integrated MANET system like: privacy, tracking, eavesdropping, skimming, cloning, replay, relay, Denial of Service (DoS), spoofing and secret disclosure attacks [44].

As an outcome of literature review (MANET and lightweight cryptography), next section presents identified research issues.

4. Identified Issues

Based on reviewed literature and experiments conducted for secure and lightweight hierarchical network construction using lightweight cryptography, the following issues require attentions:

**Issue 1:** Under the lightweight key management process of lightweight cryptography, there is lack of schemes which minimize the key generation and distribution costs and maximize the performance.

**Issue 2:** In lightweight cryptography, there is need of scenarios which integrate the cryptography primitives for maximizing the security benefits and minimizing the hardware cost. The integration of cryptography primitives should be able to achieve maximum cryptography properties.

**Issue 3:** Under hierarchical MANET construction, a lightweight model of network hierarchy is required which takes proximity of nodes into consideration for minimizing the chances of attacks and maximizing the performance benefits. Thus, lightweight protocols like identification, authentication, group formation, and tag and ownership transfer are required to be proposed.

**Issue 4:** As after the construction of MANET, authentic nodes should maximize the performance benefits by proving routing security. Thus, trust management scheme is required to be integrated for providing routing security which minimizes the energy loss and packet drop or loss. Further, it should maximize the goodput, throughput and delivery ratio.

**Issue 5:** A system is a perfectly secure system if it minimizes the chance of attacks. Thus, a probability and simulation based analysis is required to be performed for measuring the security
levels. In the MANETs, this analysis should analyze the chances of attacks in key management, group construction, distance bounding, and tag and ownership transfer processes. Further, chances of some other ad-hoc based attacks like: Sybil, eclipse and de-synchronization should be measured.

**Issue 6:** Since the lightweight system constitutes many cryptography primitives and protocols, thus there is less chance of reduction in computational and communicational costs in the formation of a hierarchical network. Hence, alternative mechanisms should be required which minimizes the cost with security aspects taken into consideration.

**Issue 7:** Integration of primitives and protocols increases the security but also increases the chances of performance degradation thus there is need to identify the parameters which maximize the performance benefits with security remain intact.

5. **Objectives of Work**

Based on literature survey and issues identified in MANET, a secure and lightweight hierarchical model is developed using ECC. MANET are constructed by extending the trust management approach in resource constrained environment with Teo and Tan protocol for key exchange using a hierarchical model and Avoine’s MA-KA2 protocol for distance bounding and mutual authentication [45][46]. These approaches are perceived as efficient lightweight approaches with strong protection against various attacks. The probability analysis shows that trust management plays an important role in improving the security of MANET. Further, network is constituted with the help of subgroups and groups. These subgroups help to form hierarchies and these hierarchies are maintained through authentication and tag and ownership transfer protocol with trust management. In summary, following are the set of objectives:

**Objective 1:** Proposed a virtual node based hierarchy for minimizing the funnel effect. Virtual nodes are not the real but programmable nodes. An extension to Teo and Tan protocol for the creation of hierarchy using lightweight key management is suggested, in which each subgroup consists of a fixed number of mobile sensor nodes. The nodes are then divided into subgroups, hierarchies, and networks to reduce the funnel effect.

The mobile sensor nodes are tracked for the establishment and maintenance of the relationship policies using trust management. After assigning identifications to nodes, communication between nodes occurs over an insecure channel; thus, there is a need for strong mechanisms to secretly exchange information.
over the channel. To achieve this, authentication protocol has been designed. Network services are administered through local and global subgroup constructions so as to save energy consumption. This goal is achieved through distance-bounding and group-yoking protocols. The process of joining and leaving nodes for right management, tag transfer, or updating some secret information is achieved through tag and ownership transfer protocols.

**Objective 2:** Lightweight primitives and protocols have been integrated with trust management cycle for providing a lightweight and secure network. In this work, trust management based fine grained access control mechanism has been designed for end users in resource constrained networks using lightweight symmetric key management in \{transmission- integrity- human factor\} and \{transmission- availability – human factor\} security pairs. Access control mechanism establishes relationships among nodes. These relationships are maintained through network policies which establish trust among nodes. Lightweight trust management based mechanism is processed through trust computation, trust propagation, trust aggregation and trust evaluation life cycles.

**Objective 3:** Proposed system has been tested against attacks and for outlier detections. A mathematical and simulation analysis of active and passive attacks is required for maximizing the security. Simulation analysis in detecting the Ad-hoc network based attacks measures the delays in proposed network hierarchy. The results show that the proposed system detects the Sybil, eclipse and de-synchronization attacks with maximum delay of 310 msec., 500 msec. and 190msec. as compared to 1.0 sec. in [47][48], 2.3 sec. in [40] and 250 msec. in [49] respectively. Probability analysis shows that the proposed scheme is protected from distance bounding protocol attacks, tag and ownership transfer protocol attacks, on-off attack and bad mouthing attack.

6. **Thesis Organization**

This work starts with introduction to MANET in chapter 1 and literature review in chapter 2. Organization of remaining chapters is as follows:

**Chapter 3** proposes an extension to Teo & Tan’s key management approach in circular hierarchical model for fixed number of group members. Teo and Tan proposed an energy-efficient generalized circular hierarchical group model, but this approach suffers from: (i) exponential increase of key messages due to dynamic topology and (ii) energy loss because of large distances among nodes in a subgroup. The proposed modification overcomes these two weaknesses of Teo & Tan’s protocol.
The exponential increase of key messages is reduced with the proposed lightweight key generation and propagation scheme, which reduces the computational and communicational costs. Location based Frisbee construction reduces the energy losses.

This ensures three properties of cryptography: confidentiality, integrity and availability. Confidentiality is ensured through lightweight encryption/decryption mechanism and integrity through lightweight hashing mechanism. An anomaly detection mechanism is proposed for ensuring availability. This anomaly detection procedure identifies the outliers in a cluster through two different processes. First process identifies the outliers in every cluster formed through proximity of nodes. Another process identifies the outliers among nodes from set of all nodes forming all clusters.

Lastly, the comparative numerical and simulation analysis of proposed approach has been made with Teo & Tan, Wen-Lin-Hwang’s (WLH) and along with Tseng’s group key agreement approach. The analysis shows that proposed approach is well suited for low computational mobile devices with minimum delay. Also, there is an improvement of 6.6 % gate equivalents (GEs) in proposed key management scheme as compared to Teo & Tan protocol. The combinations of lightweight primitives have been achieved with 11.1K to 11.8 GEs. Further, the proposed modifications make this protocol secure against replay, masquerading, spoofing, chosen ciphertext and impersonation attacks because of proper authentication and digital signatures.

Chapter 4 presents a secure and lightweight hierarchical model which provides two type of security: routing and network security. Network security is ensured through secure identification, authentication and distance bounding whereas routing security is ensured through trust management.

The problem addressed in this chapter is as follows: Let us consider a set of nodes distributed in a geographical region which form hierarchy through proximity of nodes as shown in Fig. 1. A set of nodes is divided into subgroups which have been connected through subgroup controllers and form groups. These groups are connected through Sensor-RFID reader integrated nodes and form a hierarchy. Multiple hierarchies interconnect and form a network. In a network, connectivity of nodes through proximity requires secure connection establishment thus requires secure members and communications. For a given set of nodes, the objectives are: to construct secure hierarchical Ad-hoc network constituting trusted nodes only, to integrate the lightweight identification,
authentication and distance bounding processes for providing the unique identification number, mutually recognizing the other nodes and limiting the peripheries of subgroup constituting authentic members only.

**Figure 1:** Construction of a Single-hop Hierarchical Network.

The proposed scheme uses lightweight cryptography primitives and protocols which protect the...
network from secret reveal, message repudiation, message deceit, anonymity, traceability, forward and backward secrecy, resistance to compromise and de-synchronize. The existing work does not account for all these nine parameters simultaneously but somewhat less. Further, use of ECC ensures the reliability of messages during its exchange.

Performance of the proposed scheme has been observed for different sizes of Reed Solomon ECC in quasi cyclic form in messages. The size of ECC varies from 31 to 127 bits and the results show the proposed mechanism takes less processing and transmission time as compared to Chen’s protocol [50]. Further, for 31 to 127 bits ECC the GEs required varies from 2260 to 3860 with a minimum improvement of 24.7% over Chen’s protocol [50].

Chapter 5 discusses the probabilistic, simulation and analytical analysis of active and passive attacks against proposed hierarchical model. In hierarchical model, analysis is performed for two different types of attacks viz., Distance bounding protocol based attacks and Ad-hoc network based attacks. Distance bounding protocol attack analysis includes - mafia, distance and terrorist fraud attacks. Ad-hoc network based attacks includes - bad mouthing, on-off, Sybil, eclipse, de-synchronization and slandering or promoting attacks.

The problem addressed in this chapter is as follows: Let us consider a set of nodes mutually authenticating each other for authentic group formation. These nodes mutually authenticate each other by matching the hash bit values. For a given set of any two nodes, objectives are (a) to analyze the probability of distance fraud attacks and (b) to estimate the minimum number of bits required to be matched for getting at least 50% probability with different identification numbers.

Further, automated simulation toolkits were used to estimate the time taken for detecting the Ad-hoc network based attacks. Finally, an analytical analysis of active and passive attacks was performed for measuring the security levels.

Performance of the proposed scheme has been observed for 1000 nodes for 1000 seconds using ns-3 simulation toolkits by varying the data rates (0.1, 1 and 5 pkts/sec) and packet sizes (512, 768, 1024, 2048 bits). It is found that the proposed system is protected from various attacks with better detection time compared to existing work [40][47]-[49]. For example, Sybil, eclipse and de-synchronization can be detected in less than 310msec, 500msec and 190msec. respectively which is quiet better than the earlier work [40][47]-[49]. Finally, a comparative analysis is presented between the security properties of proposed system and other schemes.
Chapter 6 presents the computational and communicational cost analysis of proposed scheme in terms of number of rounds, total number of message exchange, number of MAC operations, number of messages sent per participating node, number of messages received per participating node, size of message sent and size of message received.

The problem addressed in this chapter is as follows: Let us consider a set of nodes mutually authenticating each other for authentic group formation. Since hash based bit matching authentic mechanism is a multi round protocol which increases the computational and communicational costs exponentially with increase in number of nodes thus objectives are: (a) to identify the protocols with minimum number of rounds and propose refinements for minimizing the computational and communicational costs and (b) to measure the computational and communicational costs of proposed mechanism and compare the costs with polynomial based multi rounds authentication protocols for identifying the protocol providing maximum security at minimum cost.

In this part, 2-party based authentic group formation protocols are extended for N-party authentic group formation. Authentic group formation process discussed in chapter 4 maximizes the security levels whereas extensions to 2-party based authentic group formation minimize the computational and communicational costs.

The analytical analysis shows that for n-participating nodes, the number of rounds and total messages reduces from $\frac{n(n-1)}{2}$ and $n(n-1)$ to $n-1$ and $n$ respectively. Whereas, each of total number of MAC operations, total number of messages sent per participating node, total number of messages received per participating node, size of messages sent per participating node and size of messages received per participating node reduces to one for each participating node. Further, it also shows that although the cost of proposed multi round authentication protocol in chapter 4 is higher than 2-round authentication group formation protocols but lesser as compared to some [51]-[53] of the existing polynomial based multi round authentication group formation protocols.

Chapter 7 discusses the performance analysis of proposed hierarchical model for five routing protocols viz., Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporally Ordered Routing Algorithm (TORA), Destination Sequenced Distance Vector (DSDV) and Zone Routing Protocol (ZRP).

The problem addressed in this chapter is as follows: Let us consider a set of nodes forming the hierarchical model through subgroup formation. The objectives for the proposed hierarchical model are: (a) to identify the best routing mechanism that improves the quality of service (QoS) in terms
of delivery ratio, throughput, goodput, jitter, receiver energy dissipation and sender energy dissipation and (b) to measure the consensus establishment time in presence of attacker nodes.

Performance of the proposed scheme is measured for small and large networks with variations in number of nodes, data rates and packet sizes. The results show that ZRP protocol provides the best delivery ratio, goodput, throughput and node coverage. Also, ZRP protocol is having minimum drop rate, jitter and end to end delay. Although energy consumption of AODV protocol is lesser than ZRP but deviation of energy among nodes is least thus load is uniformly distributed over nodes in this protocol. Finally, a comparative analysis of QoS is presented between the proposed scheme and existing schemes.

Chapter 8 summarizes the conclusions drawn from the work undertaken in this thesis and proposes some future directions in which this work can be enhanced.

Keywords: lightweight, identification, authentication, group formation, tag and ownership transfer; access control policies, analysis and modeling, lightweight primitives, MANETs.

7. Conclusions

This work proposed an ECC based hierarchical and secure MANET construction mechanism. This mechanism provides two types of security: routing and network. Routing security is ensured through trust management and network security through lightweight cryptography. Teo and Tan hierarchy construction and lightweight key distribution processes are extended for network construction. Network security is ensured through an authentication, distance bounding, and tag and ownership transfer mechanisms. The proposed approaches are perceived as efficient lightweight approaches with strong protection against various attacks. The probability analysis shows that trust management plays an important role in improving the security of MANET using ECC. This probability attack analysis is checked against two protocols: Distance bounding protocol and Tag and Ownership Transfer protocol. In distance bounding protocol, probability attack analysis is performed for mafia, distance, terrorist and distance hijacking attacks. In tag and ownership transfer protocol, probability analysis of tag’s and new ownership secrets disclosure and tag impersonation attacks is performed. In both cases, fault acceptance rate of system is checked and in result it is found that system is sufficiently strong against all these attacks.

Further, the hierarchical network construction using subgroups and groups has been proposed. These subgroups help to form hierarchies and these hierarchies are maintained through authentication and tag
and ownership transfer protocol using trust management. However, increase in nodes among groups, hierarchies or network decreases the QoS of the network. Various QoS parameters taken for network performance analysis are: delivery ratio, goodput, coverage, energy consumption and jitter. In conclusion, small scale (75-nodes and 150 nodes) and large scale (1000 nodes) scenarios shows that ZRP protocol outperforms any other protocol (AODV, TORA, DSDV and DSR) for proposed security system using trust management. The proposed trust management approach is lightweight thus suitable for resource constraint networks like: MANET. For large scale network of 1000 nodes for 1000 sec., the throughput is 80 packets per second and minimum delay of 0.03 msec. These experiments show the variations of packet rates to observe the network performance with increase of traffic. Performance of routing protocols varies according to nature of routing protocol i.e. proactive, reactive, hybrid etc. Overall, ZRP performs better than other MANET routing protocols with increase in traffic.

References


