Routing Security in Open/Dynamic Mobile Ad Hoc Networks

Jameela Al-Jaroodi
College of Information Technology, United Arab Emirates University, UAE

Abstract: *Current technologies and security advances have made networked systems and applications very popular and widely used. The pervasive and practical aspects of wireless Mobile Ad Hoc Networks (MANET) made them very popular as well. This created the need for securing MANETs to provide users with authentic communications, secure and robust information exchange, and efficient security mechanisms. However, many of the security solutions devised for regular networks are not as efficient nor as effective on MANETs. This paper investigates the security issues of a common type of MANETs (open/dynamic MANET) at the network layer where routing protocols and forwarding mechanisms are used. In this paper, we identify the different security requirements specific to MANETs and survey some of the available secure routing techniques. The study has revealed some problems with the current routing protocols and identified the most important issue that needs to be resolved to ensure a secure network layer.*

Keywords: *MANET, distributed routing, ad hoc networks, security, network layer, secure routing protocols*.

Received July 13, 2005; accepted December 16, 2005

1. Introduction

Computer networks are a living necessity for almost everybody. However, they also have generated the need for sophisticated and robust security mechanisms to protect them and many have been successful in conventional networks. Currently, new technologies have emerged in the context of wireless connectivity, which are becoming popular for applications such as home and office networking and connecting mobile users. With this advancement, the need for security has also elevated, generating more research to secure wireless networks.

One of the important types of wireless networks is the infrastructureless (ad hoc) network. These networks do not have a fixed topology and do not need a centralized server to operate correctly. Ad hoc networks allow independent nodes to communicate autonomously and rely on the nodes to perform network functions such as routing and security. To add to the complexity, nodes are usually heterogeneous with varying and limited resources and are mobile. This creates the need for efficient and fast mechanisms to facilitate the connections and to provide secure routing services. In ad hoc networks, security becomes essential and complicated. Security protocols and algorithms that were used and proven in regular networks no longer satisfy the requirements in MANET. The unique characteristics of MANETs and open MANETs (as defined in section 2) created the urgent need for more sophisticated and effective solutions. Considerable research has been done and many protocols were devised to provide secure utilization of MANETs.

In this paper, we focus on the routing security in open/dynamic MANET due to the perceptible differences in requirements between this type of ad hoc networks and other wireless networks. A major problem with MANETs routing is that it is not performed by dedicated devices (routers), thus they are more difficult to monitor and secure. In addition the independence of the MANET nodes, which perform the routing, results in a more complex approach to security. This is due to the fact that nodes do not belong to a certain authority, thus can have unpredictable behavior. The network layer in a wireless network requires more secure mechanisms to prevent attacks that take advantage of the dynamic topology and the nodes' role in the process. Here we study various secure routing protocols that attempt to provide solutions to some of the security issues (described in section 3). We attempt to identify the problems in which the approaches we studied have solved and those that they did not solve.

The rest of the paper is organized as follows. The next section describes the characteristics of MANETs. Section 3 provides an overview of the security issues. Section 4 discusses the security of routing in MANETs and the open issues, while section 5 concludes the paper.

2. Mobile Ad Hoc Networks

There are various definitions for the term wireless Mobile Ad Hoc Network (MANET) as in [5, 14, 25]

and others. Ad hoc in Latin means "for this purpose only", and it implies spontaneous and temporary setting. Therefore, MANET is a collection of mobile and/or stationary devices connected through wireless links to serve a specific purpose. MANETs provide users with easier ways to connect and communicate without the need for prior setup or a centralized server. Examples of MANET applications are sensor networks (smart dust) [28], military applications [24], safety/rescue operations, conferences and meetings [8], and peer-to-peer networks. MANETs are currently used in many areas and have various defining characteristics that differentiate them from other wireless networks such as WLAN. These characteristics are:

- *Infrastructureless*: MANETs are by nature formed by independent devices wishing to communicate for some purpose and all devices have the same role.
- *Dynamic Topology*: Mobile devices move freely and could be in and out of the network dynamically, constantly changing the links and topology.
- *Low and Variable Bandwidth*: Wireless links have limited bandwidth than wires. Interference, noise and congestion effects also cause bandwidth to vary with the surrounding conditions.
- *Constrained Resources*: Generally, devices in a MANET are small handheld devices, which have limited power, processing capabilities, and storage.
- *Limited Device Security:* Devices are susceptible to physical problems such as theft, loss and damage.
- *Limited Physical Security*: Wireless links are more susceptible to external attacks on the physical layer such as eavesdropping, spoofing, jamming and Denial of Service (DoS).
- *Short Range Connectivity*: Wireless links usually have short range of transmission. This requires nodes rely on each other to perform multi-hop routing techniques to connect over large distances.

Because MANETs have a very special setting, they require a different set of security mechanisms. The absence of a centralized authority renders many of the proven security mechanisms impractical (and in many cases, useless). Most of the security mechanisms rely at some stage on the existence of a centralized authority to function correctly. New innovative mechanisms need to be devised that will work in the absence of the centralized authority and the changing topology of the network. Furthermore, MANET nodes are independent, thus do not have the obligation to behave correctly, thus mechanisms to ensure proper behavior must be considered. Among the different network layers, we view the security of the network layer as an essential aspect to the security of all above layers; therefore, it is important to provide high levels of security at this layer. More specifically, the authentication of nodes at the network layer prevents many possible attacks on the network. The major hurdle is the establishment of trust among multiple independent nodes in the absence of a trusted authentication entity.

3. Security Requirements

The security of a MANET, as in any other network, has a number of requirements that, when available simultaneously, will form a secure environment. However, the solutions are not straightforward and there is no magic combination that will make everything all right in all situations and all the time. In MANETs, these requirements are challenging to fulfill and even more difficult to support without compromising some of the unique characteristics of the MANET. The main requirements in securing a MANET are:

- *Authentication*: Authentication is essential to ensure legitimate access to the network. Nodes wishing to communicate with each other need to verify the identity of each other to be satisfied that they are communicating with the right party. This is the most difficult requirement to satisfy and the most important. Without the proper authentication, no other requirements can be correctly implemented.
- *Authorization and Accounting*: Nodes participating in a network need to have proper permissions to access shared resources on that network. In addition, in a MANET, nodes should be able to restrict others from accessing private information on their devices. Moreover, in some cases, the authorization policies are accompanied by accounting mechanisms to track resource utilization to identify bottlenecks, charging users for services or for statistical information about the network. Both authorization and accounting require robust methods to ensure correctness of protocols and proper utilization of resources.
- *Privacy and Confidentiality*: In many cases, the exchanged data, the data stored on the nodes and the location information of these devices need to be protected. Privacy implies protecting the identity and/or location of the node, while confidentiality implies the secrecy of the data being exchanged. Confidentiality can be achieved using any of the available encryption techniques, provided that proper access key systems are used. Protecting privacy involves more than encryption and requires more sophisticated techniques to hide the identity or the location of the user. This is made possible by using mechanisms to conceal the routing topology.
- *Availability and Survivability*: Availability of a network means that the network should be available to provide its services when needed even with the existence of break-ins. While survivability implies the ability of the network to provide its services

under any conditions and return the service to normal levels at normal conditions. These requirements are especially important in MANETs where break-ins, attacks and malfunctions are more frequent and less detectable.

- *Data Integrity*: When data is exchanged between network nodes, users need to be sure that it has not been tampered with or changed on transit. This is essential in situations such as banking, military operations and equipment controls (e. g., trains or planes) where such changes could cause potential damage.
- *Non-Repudiation*: A node sending a message or initiating an action on the network should not be able to deny that later. Any given node should be liable to its actions and should not be allowed to deny responsibility of these actions. This is very important in cases of disputes or disagreement over some events. This is achieved using techniques such as the digital signatures that link the data or action to the signer.

Collectively, if these requirements were fulfilled, the network should be secure against most known attacks and users will be able to form and use MANETs securely. However, achieving these requirements at the same time is very difficult and in many cases almost impossible. Research is currently focusing on each requirement separately and a few are working to integrate collections of these requirements to provide more robust protocols [18]. Regarding the design of protocols that will satisfy these requirements, several dimensions need to be considered [1]. These are cryptographic mechanisms, trust management, and heterogeneous resource management. Including these dimensions in the design helps provide secure and efficient protocols.

4. Secure Routing Protocols in MANET

Routing protocols are studied extensively for MANETs and many well-designed protocols are available. Zou discusses a number of these protocols [32], while more protocols using dominating sets routing are discussed such as [4, 7, 28, 29], and geographical-based routing [15]. In addition, much research has been done to develop secure routing protocols in MANETs; however, all require some form of initial authentication to secure the protocols. Many of these protocols are proven to provide adequate security against most attacks provided that they have that initial authentication. Here we will first discuss the different types of MANETs based on their context and applications. The three categories dictate how successful the routing protocols are and what requirements need to be fulfilled.

- *Organized*: MANETs, with well-defined purpose such as military networks in a battle field [24] and disaster relief operations, where ad hoc networks are formed between members of the teams to serve a well-defined purpose. In this situation, initial authentication is not a problem since all members belong to the same organization and share the same goals. Therefore, there is no reason for nodes to misbehave or disrupt the network. However, this type of network requires strong authorization and confidentiality measures to secure it against external attacks and compromised devices. In addition, it may be essential to conceal the locations of these nodes during operation.
- *Localized*: MANETs, semi-static ad hoc networks that are formed by devices in close proximity of each other such that they can all authenticate each other by physical contact. This type of network is also referred to as spontaneous networks [8]. In this case, initial authentication is not a problem. Nevertheless, these networks require authorization and access control mechanisms to ensure that members have access only to resources they are allowed to use. For example, an ad hoc network could be formed during a meeting between members of competitive companies. In this case, members do not want users from other companies to access their confidential organization information. Such networks can be secured using current techniques and stringent access policies.
- *Open/Dynamic*: MANETs, unstructured ad hoc networks such as those formed for temporary purposes of getting specific information or collaborating to solve a problem. An example is a number of devices in automobiles that network together to relay traffic information. Another example is sensor networks, formed among thousands of tiny sensors distributed over large geographical areas for monitoring. These networks are formed among sensors to relay data and exchange data necessary to complete their operations, but these devices can be lost, damaged or moved to different locations during their lifetime. This type of ad hoc networks is the most difficult to secure and authenticate due to the absence of a controlling authority and the independence of the devices.

In this paper, we concentrate on open/dynamic MANETs. We will investigate a number of secure routing protocols and discuss their effectiveness and the techniques used for solving the authentication problems in the absence of a centralized authority. Routing in this type of networks is based on well known techniques:

1. Distance Vector (DV) routing (proactive routing).
2. Dynamic Source Routing (DSR).
3. Cluster-based or backbone routing.
4. Geographical-based routing.

Following, we introduce some secure routing protocols and discuss their operation, advantages and weaknesses.

4.1. Proactive RSA

Although this protocol was not designed specifically for MANETs, it is a base for many other protocols used in MANETs [9]. The basic idea of proactive RSA is that it uses distributed shared keys and these keys are updated frequently to make it more difficult for an adversary to find the keys or compromise the network. The main goal is to devise a mechanism to share the key and update it without revealing the secret values (in this case Φ (N)). It is similar to the secret sharing model [10] and depends on communication through an authenticated bulletin board. The main advantages of this protocol are the prevention of jamming and the ability of nodes to reboot (re-initialize) a compromised node. However, it only provides probabilistic levels of security and requires a trusted dealer to authenticate the initial group and establish the authenticated bulletin board.

4.2. SecAODV and IDS

The authors propose a secure routing protocol (SecAODV) based on AODV and implemented over IPv6 [25]. They also include intrusion detection mechanism (IDS) that is independent from routing. The protocol requires secure binding between IP addresses and RSA keys generated by the nodes. Nodes use on-demand trust establishment and collaborate to detect malicious activities. The protocol can detect attacks like routing disruptions, resource consumption and colluding adversaries. SecAODV protects from routing disruption attacks, but cannot prevent attacks that may take advantage of MAC vulnerabilities. IDS, on the other hand, utilizes collaboration techniques to protect the network from intruding or misbehaving nodes.

4.3. SRDP

This protocol is designed to secure the route discovery process in DSR [16]. SRDP uses aggregated Message Authentication Codes (MACs) or multi-signatures. The protocol assumes bidirectional communication on each link and that a node may not know all other nodes neighboring it. The protocol also relies on the assumption that the source and destination are honest, which may not be realistic. After identifying the requirements, the authors explore several techniques to secure DSR such as forward authentication, and backward authentication, and the use of authentication tags. The design uses two tags, one generated by the source and the second is built incrementally throughout the route discovery process.

4.4. Proactive Distributed Signature (PDS) Schemes

This model provides secure routing in the absence of authenticated communications and using broadcast mediums [3]. The scheme provides a framework to convert PDS schemes that work on reliable links to equivalent PDS schemes that will work on unreliable links (links that may be controlled by an adversary). However, it requires a secure recovery protocol, which is achieved by using a read-only memory (ROM) or a smart card. The main goals here are to provide authenticity and delivery (making sure packets are delivered to the intended destination in a timely manner). This framework does not provide a specific protocol, but helps in developing secure protocols.

4.5. Authenticated Routing Protocol (ARAN)

This protocol provides secure routing for open ad hoc networks [6]. The main requirements it tries to fulfill are:

- Preventing spoofing of routing signals.
- Preventing fabrication of routing messages.
- Ensuring integrity of routed messages.
- Preventing adversaries from forming routing loops.
- Ensuring the use of the shortest routing path.
- Excluding unauthorized nodes during route discovery.
- Routing messages should not expose the topology.

The main drawback is that it requires trusted certification server to issue the initial certificates. The protocol provides two stages. The first is efficient end-to-end authentication, but does not guarantee shortest path usage and not fully secure. The second requires more CPU power and provides shortest path guarantees and stronger security. ARAN provides route maintenance mechanisms and key revocation schemes to stop compromised nodes from disrupting the network.

4.6. Emulated Centralized Certification Authority (CA)

In this protocol, a virtual centralized authority is used to issue and validate authentication certificates of the nodes [11]. It is based on public-key systems (e. g., Pretty Good Privacy (PGP)), but with a distributed CA. The private key is generated by a group of nodes and divided into shares that are distributed among multiple nodes. Any k nodes can collaborate to issue or validate a certificate, but nodes fewer than k cannot do the same. In addition, the certificate directory is also distributed. This guarantees that the private key is exposed unless an adversary gains control of k or more nodes. However, this protocol assumes that all nodes

are honest and not selfish or malicious to ensure that key shares are distributed correctly and securely.

4.7. Distributed Authentication Scheme

This protocol provides a self-securing virtual certificate authority to protect the network from DoS attacks in break-ins [19]. The main difference from the emulated CA is that it uses certificate expiration time, thus requiring periodic certificate renewal, and it maintains a distributed Certificate Revocation List (CRL) that is used to identify expired and compromised certificates. The scheme does not rely on all nodes to be honest, but it requires a mechanism to initialize the certificates (startup phase). The authors propose a number of possible solutions:

1. Using an off-line certification authority to issue all certificates.
2. Using physical identification such as biometrics (finger print or retina imprint) or smart cards.
3. Bootstrapping k nodes using an off-line certification authority. All suggested methods enforce the use of some centralized mechanism for authentication, which may be restricting and not always be possible in MANETs.

4.8. Unified Network Layer Security Solution

This solution is based on Ad hoc On-Demand Distance Vector (AODV) protocol in a fully localized approach using tokens [30]. Tokens are used as authentication certificates for the nodes. The protocol aims to provide secure routing updates and ensure packet forwarding in the presence of compromised or misbehaving nodes. The solution is composed of four stages:

1. Neighbor verification, where nodes verify their neighbors by checking the validity of their tokens. Here the expiration time of tokens increases as long as the node is behaving and participating correctly in the network; therefore reducing the need for updates.
2. Security enhanced routing protocol that is based on the tokens.
3. Neighbor monitoring, where nodes watch their neighbors to detect misbehavior or abnormal activities.
4. Intrusion reaction, where nodes react to intrusion by revoking tokens and isolating misbehaving nodes. Once more, the main problem is: Who issues the tokens?

4.9. Secure AODV

This protocol secures AODV by protecting the routing information [31]. It is based on source and end-to-end authentication using schemes like digital signatures. The protocol uses public-key schemes to protect the non-mutable data (data not required nor changed in the routing process) and uses hash chains to secure the mutable date (data necessary for the routing process), which in this case is the hop count information. The protocol requires a key management scheme and suggests a distributed CA to issue and validate certificates. The protocol works as follows: The source uses the public-key scheme to encrypt and sign the data and uses a hash function to encrypt the hop information. On the path, each router will update the hop information and use a hash function to secure it. When the message reaches the destination, it follows the same hashing chain to verify the path and uses its keys to get the rest of the data and authenticate it. This requires less CPU power from the intermediate nodes since they do not need to access the encrypted data. Nonetheless, it cannot protect the network from the tunneling attack. In addition, it still requires some authority to provide the nodes with valid (trusted) certificates.

4.10. Secure Routing Information

This protocol is similar to the Secure AODV, but is based on the DSR protocol [24]. It assumes a security association between the source and destination via a trusted key-pair and a reliable physical/link layer services. The source initiates a route discovery request and relies on the signed reply from the destination to verify the discovered path. This method protects the network from IP spoofing (a node impersonating another by stealing its IP address) and from false routing information since the source will only trust a full path provided by the destination. The problem here is establishing the security association between the source and destination, which requires a trusted key-pair that needs to be issued by a trusted CA.

4.11. Secure Efficient Ad Hoc Distance Vector (SEAD)

This protocol enhances the Destination Sequenced Distance Vector (DSDV) protocol to protect against DoS attacks [12]. It uses efficient one-way hash functions to reduce the overhead and speedup the routing process. It also assumes a limited network diameter to reduce the amount of information needed in the routing table and the number of hops in any given rout. As in secure AODV, it uses incremental hashing of the route information to obtain a correct path to the destination. It also requires a similar security association between the source and destination. This creates the same problem of having to rely on some CA to provide this association.

4.12. Distributed Key Shares

This protocol uses distributed key shares, as in proactive RSA, and utilizes periodic share updates [16]. It also supports node reboot (to recover a

compromised node) and distributed new-member authentication. In addition, it provides mechanisms for both implicit and explicit certificate revocation. Implicit revocation occurs with the expiration of a certificate (when a node is denied a renewal of its certificate), while explicit revocation is done by maintaining a CRL to identify and isolate compromised nodes. This scheme provides authentication, integrity and availability in the network. To ensure security, nodes need to have some form of tamper-proof component that will hold its valid certificate and identification information. However, it also requires initial authentication of startup nodes.

4.13. Ariadne: On-Demand (Reactive) Routing

This protocol, based on dynamic source routing (DSR), uses symmetric source routing and prevents DoS and route tampering [13]. It can be used in conjunction with different mechanisms, such as:

- Public-key infrastructure, in which pre-established keys are needed for digital signatures.
- Shared secret keys that are setup beforehand with TESLA (an efficient broadcast authentication schemes requiring loose time synchronization). In this case time stamps are used to validate keys.
- Secret keys that are pre-established from encryption.

The protocol assumes nodes will only trust themselves and the destination node for path authentication. Using this protocol can also protect against blackhole attacks, where a compromised node drops all the packets it receives. This is achieved because paths are only authenticated by the destination; therefore, dropped packets will cause the nodes dropping them to be excluded from the paths.

4.14. CORE: Collaborative Security Mechanism

This scheme provides a mechanism to force nodes to cooperate in the route discovery process and in forwarding packets [21, 22, 23]. It is based on DSR and secures both the route discovery and route maintenance phases. The protocol uses a reputation mechanism where each node is assigned a reputation value. When a node cooperates, its reputation value increases; while misbehaving nodes are penalized by reducing their reputation. Nodes maintain knowledge of the reputation of their neighbors and use that information when selecting routing paths. In addition, nodes with "bad" reputation are denied services when they require sending packets. The reputation value is hard to increase, but easier to decrease, making it undesirable for nodes not to cooperate in fear of being denied service. The approach protects the network from selfish and malicious nodes. Nevertheless, it requires a trusted initialization method like tamper-proof devices.

4.15. Watchdog and Pathrater

This protocol is also based on DSR and provides secure routing and protection from selfish and misbehaving nodes [20]. It provides two mechanisms that jointly achieve this goal. The watchdog is used to monitor neighboring nodes to make sure they are performing their jobs (forwarding packets). This is made possible by the nature of the wireless transmission, since any node in the proximity of another can hear its transmissions. Since DSR provides full path information and a node knows where the next hop (its neighbor) should forward the packet. It listens to the neighbor's transmission to make sure it has forwarded the packet to the correct node. If it detects that the node did not forward the packet or sent it to a different node, it will report this to the source. The pathrater assigns rate values to links used, based on how well the nodes connected to it cooperate. These values are then used to determine the best path to route new packets. This path may not be the shortest path in the network, but its rate is the best.

4.16. Enforcing Cooperation

This scheme is used to encourage nodes to cooperate and forward packets for other nodes based on having counters associated with each node [1]. The counters are incremented when a node cooperates by forwarding a packet and decremented when the node sends a packet for itself. These counters need to be protected from malicious activity to prevent nodes from adding credit to itself or decreasing other nodes' credit. This protection requires a number of measures to be taken. First, the credit accounting and packet forwarding mechanisms need to be secured in tamper-proof devices such as a smart card. In addition, these cards need to have security key-pairs to be used in the protocol. All nodes need to keep the public keys of all other devices in order to ensure secure communication and credit updates. However, with large networks this becomes more difficult because the number of keys used will be very large. The authors propose a solution to the problem by limiting the number of manufacturers of the tamper-proof devices such that all devices coming from the same manufacturer will have the same key-pair. However, this will restrict the number and type of devices that can participate in the network.

4.17. Discussion and Open Issues

The protocols discussed provide secure routing for mobile ad hoc networks using different mechanisms. They all provide additional features to existing routing protocols designed for conventional networks to

achieve security in MANETs. The enhanced protocols provide security against many attacks such as Denial of Service (DoS), Distributed DoS, message replay, route tampering, wormhole and blackhole attacks. In addition, some protocols protect against internal node selfishness and misbehavior. Few others provide innovative mechanisms to motivate selfish and misbehaving nodes to be more cooperative and participate responsibly in the routing and packet forwarding operations. These mechanisms rely on the general concept of virtual currency or reputation. All of the studied protocols and security schemes provide good levels of security, but at the same time, they have some problems that may make them difficult to apply in MANETs. Some problems are:

1. *The use of public-key cryptography*: The encryption algorithms are CPU intensive, which may not be suitable for many devices in the MANET, such as cell phones and PDAs. In addition, using public-key encryption is time consuming, thus protocols that use them in all stages suffer delays in the routing and packet forwarding process. However, a few algorithms use this technique only for the initialization phase or for securing non-mutable information only. Moreover, public-key encryption, requires secure key management and distribution mechanisms (through a centralized or distributed certification authority) that may not always be available in a MANET.
2. *The use of tamper-proof hardware*: Although this method looks secure and efficient, not all devices support their use. In addition, these devices, like any other device, can be lost or stolen, so users could be locked out from using their own devices. Moreover, these devices need to be initially authenticated and linked to their owners and all other devices need to verify this ownership to be able to trust the owner.
3. *The use of incremental hash functions*: Hash functions are very efficient and secure, but the need for a shared secret key makes it very difficult to apply in a MANET, where there is no perfectly secure way to exchange the secret key without either physical association or a trusted third party. Some protocols use public-key encryption to secure the key exchange process, but this takes us back to the first problem: Who issues and verifies the public-key pairs needed.

A close examination of the problems mentioned reveals one major issue that needs to be addressed in order to make these protocols more feasible and more suitable to MANETs. As describes earlier, one of the main characteristics of MANETs is the lack of a well-defined infrastructure and centralized authority. All proposed protocols require some arrangement to provide the initial trust between all the nodes or in some cases some of the nodes in the network. Therefore, to secure any routing protocol in a MANET, a fully localized, self-managed protocol is needed. Such protocol provides robust, scalable and efficient distributed model to authenticate nodes and to secure routing by establishing the authentication of participating nodes. In addition, efficient algorithms are needed to reduce the CPU, communication and storage requirements. This introduces multiple constraints on the possible mechanisms that can be utilized. For example, it will not be feasible to use a centralized certification authority and it will also be difficult to support public-key encryption mechanisms for all security purposes since this cannot be supported by low processing/power devices. The issue of initial trust is the key to solving the security problem at this layer; however, it is also an undecidable problem. Therefore, attempting to find an absolute answer is not a realistic venture. Protocols and mechanisms that can provide relatively acceptable levels of trust without imposing too many assumptions on the MANET are needed. As an analogy, a signature is accepted as a binding authentication of identity of the signer; however, it can still be forged. What is needed is a scheme that will provide a level of trust comparable to that of a physical signature.

5. Conclusion

In this paper, we discussed the security issues in MANETs at the network layer. To provide a good understanding of the issues, we started with a general overview of the network security, mobile wireless networks and the security requirements for MANETs. The study focused on the network layer and the security of the routing protocols. Due to the fact that many of the security protocols realized at the higher levels assume secure and robust routing in the network. In addition, the security protocols at the transport and application layers share the same general principles in regular, wireless and ad hoc networks. However, unlike in regular networks, where specially designed routers and switches are used, MANET devices have to perform this task for each other. This creates the possibility of having selfish and misbehaving nodes in addition to compromised and impersonated nodes. To ensure the correct operations of the MANET, it is essential to have correct and secure routing mechanisms.

The study introduced many secure routing protocols and discussed their strengths and weaknesses. We identified a number of potential problems such as the use of public-key encryption, the difficulty to securely exchange symmetric encryption keys, and the assumption of existing trust between nodes. Nevertheless, the main problem common to most protocols is the need for an initial establishment of trust among some or all nodes in the network. However, we also recognize the difficulty of achieving such trust within the context of a MANET. Most

protocols do not provide a complete solution that fully matches the infrastructureless nature of MANETs. The most important issue that we believe needs to be addressed is to answer the question: "How could a collection of independent nodes wishing to form a MANET trust each other in the absence of trusted authentication authority?" The answer will provide the break-through needed to boost the popularity and efficient utilization of MANETs. We propose further investigation of the authentication issue such that we can guarantee trust among the minimum set of nodes required to successfully establish the routing process. Our next step is to investigate successful protocols currently used in other networks and adapt some efficiently to satisfy the open ad hoc networks requirements for security. One of the promising approaches is the utilization of collaborative techniques to enhance the process.

References

[1] Balakrishnan V. and Varadharajan V., "Designing Secure Wireless Mobile Ad Hoc Networks," *in Proceedings of IEEE International Conference on Advanced Information Networking and Applications*, Taiwan, March 2005.

[2] Buttyan L. and Hubaux J. P., "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," *ACM Journal for Mobile Networks (MONET)*, Special issue on Mobile Ad Hoc Networks, 2002.

[3] Canetti R., Halevi S., and Herzberg A., "Maintaining Authenticated Communication in the Presence of Break-ins," *Journal of Cryptology*, vol. 13, no. 1, pp. 61-105, 2000.

[4] Cardei M., Cheng X., and Du D. Z., "Connected Domination in Multihop Ad Hoc Wireless Networks," *in Proceedings of the 6th International Conference on Computer Science and Informatics (CS&I'2002)*, North Carolina, March 2002.

[5] Corson S. and Macker J., "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," *RFC 2501*, available at: http://www.ietf.org/rfc/rfc2501.txt, January 1999.

[6] Dahill B., Levine B. N., Royer E., and Shields C., "A Secure Routing Protocol for Ad Hoc Networks," *Technical Report*, UM-CS-2001-037, U. Mass Amherst, August 2001.

[7] Das B., Sivakumar R., and Bharghavan V., "Routing in Ad Hoc Networks Using a Spine," *in Proceedings of International Conference on Computer Communications and Networks*, September 1997.

[8] Feeney L. M., Ahlgren B., and Westerlund A., "Spontaneous Networking: An Application-Oriented Approach to Ad Hoc Networking," *IEEE Communications Magazine*, vol. 39, no. 6, pp.176-181, June 2001.

[9] Frankel Y., Gemmell P., MacKenzie P. D., and Yung M., "Proactive RSA," *in Proceedings of CRYPTO'97*, Springer Verlag, LNCS, pp. 440-454, 1997.

[10] Herzberg A., Stanislaw, Krawczyk H., and M. Yung, "Proactive Secret Sharing or How to Cope With Perpetual Leakage," *in Proceedings of CRYPTO'95*, Springer Verlag LNCS 963, pp. 339-352, 1995.

[11] Hubaux J. P., Butty´an L., and Capkun S., "The Quest for Security in Mobile Ad Hoc Networks," *in Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Long Beach, CA, USA, October 2001.

[12] Hu Y. C., Johnson D. B., and Perrig A., "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *in Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02)*, NY, June 2002.

[13] Hu Y. C., Perrig A., and Johnson D. B., "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *in Proceedings of MobiCom'02*, Atlanta, Georgia, USA, September 2002.

[14] IETF on Mobile Ad-hoc Networks (MANET), "Description of Working Group," Official Charter, available at http://www.ietf.org/html.charters/manet-charter.html, 2005.

[15] Jain R., Puri A., and Sengupta R., "Geographical Routing Using Partial Information for Wireless Ad Hoc Networks," *Technical Memo*, UCB/ERL M99/69, December 1999.

[16] Kim J. and Tsudik G., "SRDP: Securing Route Discovery in DSR," *in Proceedings of the International Conference on Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous'05)*, San Diego, California, July 2005.

[17] Kong J., Zerfos P., Luo H., Lu S., and Zhang L., "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," *in Proceedings of IEEE International Conference on Network Protocols*, Riverside, CA, November 2001.

[18] Levijoki S., "Authentication, Authorization and Accounting in Ad Hoc Networks," *Technical Report*, Helsinki University of Technology, available at: www.tml.hut.fi/Opinnot/Tik-110.551/2000/papers/authentication/aaa.htm, May 2000.

[19] Luo H., Zerfos P., Kong J., Lu S., and Zhang L., "Self-Securing Ad HocWireless Networks," *in Proceeings of 7th International Symposium on*

Computers and Communications (ISCC'02), Taormina, Giardini Naxos, Italy, July 2002.

[20] Marti S., Giuli T. J., Lai K., and Baker M., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*," in Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 255-265, 2000.

[21] Michiardi P. and Molva R., "Game Theoretic Analysis of Security in Mobile Ad Hoc Networks," *Research Report*, no. RR-02-070, Institut Eurécom, France, April 2002.

[22] Michiardi P. and Molva R., "Making Greed Work in Mobile Ad Hoc Networks," *Research Report*, no. RR-02-069, Institut Eurécom, Sophia-Antipolis, France, March 2002.

[23] Michiardi P. and Molva R., "Prevention of Denial of Service Attacks and Selfishness in Mobile Ad Hoc Networks," *Research Report*, no. RR-02-063, Institut Eurécom, Sophia-Antipolis, France, January 2002.

[24] Papadimitratos P. and Haas Z. J., "Secure Routing for Mobile Ad Hoc Networks," *in Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS'2002)*, San Antonio, TX, January 2002.

[25] Patwardhan A., Parker J., Joshi A., Karygiannis A., and Iorga M., "Secure Routing and Intrusion Detection in Ad Hoc Networks," *in Proceedings IEEE International Conference on Pervasive Computing and Communications*, Hawaii, March 2005.

[26] Shrader B., "A Proposed Definition of 'Ad Hoc Network'," *Report*, Royal Institute of Technology (KTH), available at: http://www.old.s3.kth.se~brooke/Reports/pscience.pdf , 2002.

[27] Sterbenz J. P.G. and Krishnan R., "Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions," *in Proceedings of Mobile Ad Hoc Networks (WiSe'02*), Atlanta, GA, September 2002.

[28] Warneke B., Last M., Liebowitz B., and Pister K. S. J., "Smart Dust: Communicating with a Cubic-Millimeter Computer," *Computer*, vol. 34, January 2001.

[29] Wu J., "Dominating-Set-Based Routing in Ad Hoc Wireless Networks," *in Wireless Networks and Mobile Computing*, Stojmenovic I. (Ed.), John Wiley & Sons, pp.425-450, 2002.

[30] Yang H., Meng X., and Lu S., "Self-Organized Network-Layer Security," *in Proceedings of Mobile Ad Hoc Networks (WiSe'02)*, Atlanta, Georgia, USA, September 2002.

[31] Zapata M. G. and Asokan N., "Securing Ad Hoc Routing Protocols," *in Proceedings of ACM Workshop on Wireless Security*, Atlanta, GA, pp. 1-10, 2002.

[32] Zou X., Ramamurthy B., and Magliveras S., "Routing Techniques for Wireless Ad Hoc Networks-Classification and Comparison," *in Proceedings of 6th World Multi-conference on Systemics, Cybernetics, and Informatics-SCI*, July 2002.

Jameela Al-Jaroodi received her bachelor degree from The University of Bahrain in 1993, her master degree from Western Michigan University in 1998, and her PhD from the Computer Science and Engineering Department at the University of Nebraska-Lincoln in 2004. Currently, she is working as a research assistant professor at the Department of Electrical and Computer Engineering, Stevens Institute of Technology, NJ, USA. She published more than 30 articles in journals and conferences. Her research interest is in distributed systems, which includes middleware, distributed software for heterogeneous systems, ad-hoc networks, sensor networks, and software engineering for distributed systems.