A survey on security in Mobile Ad Hoc Networks

Åsmund Ahlmann Nyre
SINTEF ICT,
Trondheim, Norway
Asmund.A.Nyre@sintef.no

Abstract

Mobile ad hoc networks (MANETs) has for several years been viewed as a promising technology for several application areas where fixed infrastructure is either unreliable or non-existent. Although the technology has been around for quite some time it has yet to become widely deployed. There may be several reasons for this, however a contributing factor is the lack of agreed upon security mechanisms for MANETs, making it difficult for users and organisations to specify the desired level of protection. In this paper we describe proposed security mechanisms and discuss how they fulfil the high level security goals of availability, confidentiality, integrity, authentication and non-repudiation. Based on this discussion we also point out important areas for further research.

1. Introduction

Mobile ad hoc networks (MANETs) has for several years been viewed as a promising technology for several application areas where fixed infrastructure is either unreliable or non-existent. This includes government areas such as military tactics operations, emergency and rescue operations, crisis management, and commercial applications such as conference venues, ad hoc gaming or extending wireless coverage. Although the technology has been around for quite some time it has yet to become widely deployed. One important factor is the ability to secure MANETs. While routing protocols have been standardized (e.g. [1]–[3]) security extensions have not. With wireless access network such as the IEEE 802.11 [4] protocol standard link encryption schemes have been included such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2/RSN (Robust Security Network), allowing users to specify the level of protection they require. MANET security has not yet matured to this state, which may be seen as one of the reasons for the limited deployment.

Security requirements will naturally vary depending on its usage; such that MANETs for military tactics operations require more protection than an ad hoc gaming network. However, previous work [5] have outlined availability, confidentiality, integrity, authentication and non-repudiation as the main security goals to consider for MANETs.

Availability means to ensure that the network is operative whenever it is needed. With focus on intentional faults (i.e. attackers), availability implies protection, detection and recovery from denial-of-service (DoS) attacks. The principle way of achieving such attacks is by distorting routing table calculation (link fabrication, hop count manipulation, wormholes, etc.) or by flooding the network to consume bandwidth. Confidentiality implies protecting the network content (e.g. routing table updates) from unauthorized disclosure. In particular for military, emergency and crisis management operations it may be vital not to disclose the network participants to the outside world. Integrity ensures that data has not been altered during transmission, either intentional or unintentional. Authentication allows node to verify the identity of its peers, preventing nodes from acting on behalf of another. Non-repudiation means that nodes cannot deny transmitting a message. In this paper we describe proposed security extensions to MANET routing protocols and discuss how they fulfil these high level goals.

The remainder of this paper is organised as follows; in Section 2 we provide an overview of three popular MANET routing protocols for which security protocols have been proposed, to give a basic understanding of their working. In Section 3 we describe proposed proactive security protocols that reduces the likelihood of compromise. The reactive security protocols (intrusion detection mechanisms) seeking to detect and react to misbehaving nodes are described in Section 4. Next, in Section 5, we discuss how the protocols meet the security goals listed above and identify unresolved issues before we give our concluding remarks in Section 6.

2. Routing protocols

Attempts to secure routing in MANETs have mostly been done by specifying extensions to the original unsecured routing protocols. We therefore will in the following give an overview of the main classification of MANET routing protocols, before we briefly outline the main characteristics of three popular such protocols.

MANET routing protocols either perform route discovery proactively or reactively. Proactive route discovery protocols utilizes beacon messages, i.e. messages that are transmitted periodically, to inform other nodes of current routes in the network. Thus, whenever a node needs a route to a destination, it is already available and no additional delay is introduced. The problem with this approach is that control data overhead may be significant due to the periodic flooding of routing information, particularly for dense networks and networks with few transmissions. Also routing tables may be quickly outdated for rapidly moving nodes. MANET protocols based on reactive route discovery does not utilize any periodic dissemination of routing information, but instead floods the network for a route to a destination whenever this is needed by the node. Thus, there is no control data overhead as long as the network is idle and consequently reduced risk of congesting the network with such control data. The problem is however that if a link in an established route breaks, the entire route discovery process must be re-initiated, which may cause a significant delay in packet delivery. However for networks with little node movement, this will rarely happen and hence the overhead is greatly reduced compared to the proactive approach. There are several factors that need to be considered to determine which of the two approaches are better, including node movement, network density, area size (average hop-count), bandwidth, network load, etc.

The Destination Source Routing (DSR) protocol [1], [6] is a reactive protocol where the entire route to the destination is listed in each packet. Route discovery is done through broadcasting route request messages containing the destination address. The request is propagated through the network with all intermediate nodes adding their address to the route stored in the packet, until either the destination or a node with a route to the destination is reached. A route reply is then sent either using the reverse path of the request, or preferably piggybacked on a new route request to the initial sender. Piggybacking is considered better since links may be asymmetric and hence the reversed route may not be valid. Route maintenance is performed either actively through the reception of link-layer acknowledgements or passively through detecting the receiving node's retransmission in promiscuous mode. Detected link errors, i.e. missing acknowledgements, results in the transmission of a link error message to the sender. Similar to route reply, this may either be done through the reverse path of the current route or preferably piggybacked on a route request to the sender. To improve efficiency, DSR also allows nodes to utilize promiscuous mode to discover routes and errors handled by adjacent nodes.

Ad hoc on-demand distance vector routing (AODV) [2], [7], is a reactive protocol similar to DSR. AODV however does not carry the entire path in the packet header, instead each intermediate node independently computes the optimal next-hop for the given destination. Route discovery is performed by flooding route requests (RREQ) in the network to reach either the destination or an intermediate node with a valid route to the destination. The next-hop in the reverse path, i.e. the node from which the RREQ was received, is recorded by every intermediate node. Upon reaching the destination (or another node with a valid route) a route reply (RREP) message is unicast back along the the recorded reverse path. Intermediate nodes receiving a RREP records the forward path, i.e. the node from which the RREP was received. Timers are associated to the routing table entries such that invalid or unused routes are removed after a predefined period of time. AODV is said to be "a pure on-demand route acquisition system" [7], meaning that unless nodes lie on an active path (i.e. route), it does not have to maintain or advertise any routing information.

The Optimized Link State Routing (OLSR) protocol [3], [8] is a proactive protocol that actively maintains routes to all destinations in the network by periodically transmitting control information. Local link sensing is achieved by broadcasting HELLO messages containing every one-hop link known to the node. The receiver is then able to compute its two-hop neighbour set, which in turn allows it to create a Multi-Point Relay (MPR) set. The MPR set is formed such that it includes the least number of one-hop neighbours such that every two-hop neighbour can be reached. The protocol specifies that only neighbours belonging to the MPR set is allowed to forward control messages on behalf of a node. Thus, the cost of flooding control packets in the network is considerably reduced. Topology information beyond the two-hop neighbours already known using HELLO messages, is distributed using Topology Change (TC) messages. Every node maintains a MPR Selectors set containing all nodes that have selected it as MPR. Every node with a none-empty MPR Selectors set must periodically flood the network (using MPR) with TC messages containing at least every node in the MPR Selectors set. One may extend the TC messages to include additional nodes and also create suboptimal MPR sets, however at the cost of increased overhead and consequently reduced performance.

3. Secure MANET routing

The Ariadne [9] is a secure on-demand routing protocol based on DSR. It provides three ways of authenticating routing messages; using pairwise shared secret keys, using pairwise shared secret keys combined with broadcast authentication or digital signatures. If shared keys or digital signatures are used then the routing message is authenticated by appending a Message Authentication Code (MAC) or digital signature for each intermediate node. The protocol also proposes the use of TESLA broadcast authentication mechanism [10] for intermediate hop authentication and shared secret for endpoint authentication. The TESLA mechanism utilizes reversed hash chains and delayed key disclosure to provide authentication of routing messages. The protocol requires loosely synchronised clocks and a delay of at least the network round-trip time to guarantee that the message has been received by all nodes before the key is disclosed. Ariadne provides both integrity and authentication of routing information, however non-repudiation can only be guaranteed when using digital signatures, since MACs are impossible for others to verify.

The Secure Routing Protocol (SRP) [11] is designed as an extension to DSR or the inter zone part of the Zone Routing Protocol (ZRP) [12]. The protocol relies solely on symmetric key cryptography for authenticated route discovery, assuming that a shared secret keys have already been established between the source and destination nodes. A Message Authentication Code (MAC) based on the shared key is appended to route requests in order to allow the destination to authenticate the originator. However, intermediate nodes and the recorded route are not authenticated. Additionally, route error messages do not contain any verification and hence can be forged by adversaries. The protocol provides authentication and integrity, but introduce some serious issues for the availability.

The Secure AODV routing protocol (SAODV) [13] utilizes hash chains for authenticating mutable data in route request messages. However for non-mutable data the protocol uses only digital signatures. A node requesting a route to a destination generates a random seed for the hash chain and computes the maximum hash chain value by repeated hashing of the seed until reaching the maximum hop count. The signature on all fields but the seed and hop count is appended to the message. Intermediate nodes verify the signature and that the maximum hash chain value is reached after hashing the received seed (max_hop_count-hop_count) times. If verification holds, the hop count is stepped and the seed is updated by hashing it. In order to allow intermediate nodes to respond with a RREP whenever it holds a valid route in its route cache, the double signature scheme is proposed. Route error messages do not use the hash chain mechanism, but is instead digitally signed. Since it is not considered relevant which node initially started the error message, the signature is replaced for each hop, rather than appended. The protocol provides authentication for end nodes, but not for intermediate, allowing adversaries on the path to forge their identity. The hash chain mechanism guarantees that malicious nodes cannot reduce the hop count value, but may increase it or omit updating it.

Authenticated Routing for Ad hoc Networks (ARAN) [14] is a signature-based extension to the AODV routing protocol, providing secure route discovery. Route requests are signed by the originator of the request and propagated throughout the network. Intermediate nodes will, upon receiving the request, verify the signature and the sequence number before adding their signature and forwarding it to their neighbours. The destination validates all signatures and creates a signed route reply message including the sequence number and source of the request. The reply is sent back to the source along the reverse path of the request, where intermediate nodes verifies and signs it in the same manner as the request. Link failures are detected and reported using routing error messages, which are signed by the reporting entity and propagated through the network. No intermediate node signs the error message. The proof-of-concept implementation and subsequent testing indicates that the protocol increases the delay for route setup by several orders of magnitude. The tests done on the protocol shows that even with fairly powerful laptops, the ARAN protocol using 1024 bits RSA keys are approximately 23 times slower than the unsecured AODV protocol [14].

The Secure Link State Protocol [15] is a secure proactive routing protocol employing a similar strategy as SAODV for message authentication. Link State Updates (LSUs) are digitally signed by the originating node, with all mutable fields excluded. The mutable fields are instead governed by a hash chain, which do not allow reduction in the hop count. By specifying a maximum hop count, the protocol can be used as the intra zone part of ZRP [12] Only end-nodes are authenticated, such that intermediate nodes may spoof their identity without being revealed.

4. Intrusion detection

Given the lack of network perimeters and the open collaborative nature of mobile ad hoc networks it is hard to define what actually constitutes a network intrusion. Commonly, intrusions are viewed as malicious behaviour aimed at disrupting or degrading network performance.

The WATCHERS protocol [16] was proposed to enable detection of disruptive nodes in the network. The idea is to use conservation of flow, i.e. what comes in must come out, to detect misbehaving nodes. Every node monitors its neighbours and measures the amount of dropped packets, misrouted packets, etc, by listening to the communication of adjacent nodes and comparing received packages to the transmitted ones. If metrics exceed a predefined threshold, the corresponding node is considered malicious and the link to it dropped. The protocol has been criticised for its assumptions on the reliability of wireless communication [17], since there are numerous valid reasons for dropping a packet.

A similar detection and prevention scheme was proposed by Marti et al. [18] where a *watchdog* is used to detect misbehaving nodes and a *pathrater* is used to compute paths avoiding the detected nodes. Designed for the DSR protocol, the watchdog mechanism utilizes promiscuous mode and knowledge of the path to the destination to assert whether the neighbour node actually forwards packets as expected. A counter is increased whenever a routing misbehaviour is detected, ultimately blocking the node if the counter reaches a predefined threshold. Unlike the WATCHERS protocol, watchdog and pathrater are protocol specific so as not to rely solely on the conservation of flow as a detection mechanism.

The COllaborative REputation mechanism (CORE) [19] like the previous protocols also utilizes a watchdog mechanism and additionally includes a reputation system. The reputation system specifies three different types of reputation; subjective, indirect and functional. Subjective reputation is based on direct observation through the watchdog mechanism operating in promiscuous mode. Indirect reputation is based on received reputation metrics from other nodes, while functional reputation indicates the reputation for a particular functionality (e.g. packet forwarding). To prevent denial-of-service attacks by malicious broadcasting of negative ratings for benign nodes, indirect reputation may only take positive values. Unlike the *watchdog/pathrater* approach described above, CORE does not exclude malicious nodes from routes, but rather encourages cooperation in order to receive network services.

The DSR protocol extension CONFIDANT (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks) [20] consists of a monitor, a trust manager, a reputation system and a path manager. The monitor is similar to the watchdog mechanism and performs local detection of misbehaviour. The trust manager is responsible for distributing ALARM messages regarding malicious behaviour to nodes belonging to a friends list. It also computes trust levels of received information such that weighting may be employed for rating changes. The reputation system provides a quality rating of participating nodes, based on local and received information. Sufficient evidence must be gathered before a decision is made and it must have been gathered over a long enough time to rule out coincidence. The path manager is responsible for rating the active paths in the network and to react to paths containing malicious nodes (e.g. delete the path).

is similar to the watchdog/pathrater approach, but additionally creates incentives for correct behaviour of nodes by refraining from forwarding packets on behalf of misbehaving nodes. The CONFIDANT protocol proposes the use of a trust manager to share its ratings with the other nodes in the network. Route selection is done according to a trust metric such that the most trusted path is selected. If there is more than one path with highest trust rating, the shortest is selected.

The strategy by Wang et al. [21] is to use protocol specific properties for sanity checking routing updates. For the OLSR protocol, the use of multi-point relays (MPRs) allows some checking of the originating node. For example; If node A advertises a link to node B, then node A must be an MPR of node B. Thus, node B can perform a sanity check of the received information by comparing the originator to its set of MPRs. Wang et al. [21] further proposes for B to broadcast (through its MPRs) a message to invalidate the advertised link, so that other nodes will refrain from using it. There are several such properties that may be used to verify the correctness of the advertised information. The article does not discuss other reasons for such incoherence, such as latency in TC updates, link failures, etc, nor what actions should be taken upon receiving an invalidation of a link. Labelling the originator as malicious would introduce the possibility for malicious nodes to emit invalidations randomly to its MPR nodes and thereby convince the network that the benign node is malicious. If the check was performed by any adjacent node to B (i.e. in B's HELLO set) or any of B's MPRs, a majority vote could be used to guarantee the correctness of the invalidation.

Otrok et al. proposes a different strategy for intrusion detection that greatly reduces power consumption of participating nodes [22]. The idea is to let nodes in a cluster elect one single node to perform intrusion detection on behalf of the others in a collaborative game, maximising the security for the network as a whole. In order to mitigate the risk of having a misbehaving node performing the intrusion detection a set of checkers are simultaneously elected to verify correct behaviour. By sampling the communication, the checkers collaboratively decide through majority vote whether the elected node is misbehaving. For this approach to be valid, at least half of the checkers must be benign in order to guarantee that no benign node is blocked from the network. Although the approach is favourable in terms of energy consumption, networks of highly mobile nodes may force constant re-elections of both intrusion detection nodes and checkers. While obviously degrading performance and throughput of the network, this may also hamper detection of misbehaving nodes as it is impossible to gather sufficient information for making a decision before a re-election is done.

Another approach to reduced energy consumption is to for each node to only have its intrusion detection mechanism running a portion of the time [23]. They develop a game theoretic approach to model how the defender and attacker choose the percentage of the time the defence and attack will be running, respectively. By assuming different detection rates, the game is simulated to show the impact of reduced monitoring.

5. Discussion

In the previous sections we have given an overview of preventive and reactive security mechanisms tailored for use in MANETs. The next step would be to identify the missing parts (if any), in order to provide secure MANETs. Referring to the security goals identified in Section 1, we need to map each of the protocols to whether they provide authentication, confidentiality, integrity, authentication and nod-repudiation.

For reactive protocols aimed at detecting misbehaving nodes, there is typically no cryptographic support that enables confidentiality, authentication and non-repudiation. Integrity could be supported by observing neighbours' retransmissions, however the key property of such protocols is availability. By detecting and reacting upon misbehaving

Protocol	Availability	Confidentiality	Integrity	Authentication	Non-repudation	Assumptions
Ariadne	Yes	No	Yes	Yes[a]	No[b]	Established PKI or shared secret keys
SRP	Yes	No	Yes	Yes[a]	No	Established shared secret keys
SAODV	Yes	No	Yes	Yes[a]	Yes	Established PKI
ARAN	Yes	No	Yes	Yes	Yes	Established PKI
SLSP	Yes	No	Yes	Yes[a]	Yes	Established PKI

a. Not intermediate nodes

b. Unless using digital signatures

Table 1. Comparison of proposed secure MANET protocols

nodes the probability of correct functioning of the network is improved. Thus, when identifying whether the protocols meets the security goals, we have only included the preventive protocols. Table 1 summarizes how the various protocols meet the security goals. Note that the availability property is considered satisfied if the protocol *improve* denial-of-service resistance and does not imply that it will resist all attacks. Also, the non-repudiation property is not considered satisfied when using hash-chains or symmetric key MACs for message authentication. Hash chains only provide temporal evidence, since after key disclosure anyone can create authentic messages. MACs on the other hand are not verifiable to anyone but the entities that share the secret key, and does not provide evidence as to which of these entities initiated the message. What is perhaps most noteworthy is the fact that none of the protocols provide any confidentiality of routing information. For general purpose MANETs with free access, confidentiality may seem unnecessary. However, for closed networks such as military, rescue or crisis management MANETs, it may be vital that outsiders cannot identify network participants and also are unable to build a network map. Thus, for such applications of MANETs, there should be a protocol to provide this. Note also that all protocols either rely on an established MANET-wide PKI or pairwise shared secret keys. Although there exist numerous key management and key sharing schemes [5], [24], [25], this is not trivially achieved, especially for open commercial applications areas such as a conference venue.

There are of course other non-security properties to consider such as data and processing overhead, battery consumption, delay, etc., which influence the choice of security mechanism. For instance, the extensive use of digital signatures in the ARAN protocol ensures a higher level of security (e.g. secure authentication of intermediate nodes) at the cost of added processing and data overhead for each hop. Thus, the optimal protocol is not necessarily the one providing the optimal security.

As with conventional intrusion detection systems, detecting misbehaving nodes in MANETs may be erroneous, which in turn may have devastating effects on the Network. Since availability is the primary goal of such systems, labeling a benign node as malicious would in effect constitute a denial-of-service attack by the protocol. Similarly if malicious nodes are undetected, the availability of the entire network would be threatened.

The protocols and mechanisms outlined in Section 4 all uses anomaly based detection, where deviations from correct protocol behaviour is considered malicious. Additionally, all protocols rely on obtaining information by promiscuously overhearing neighbour transmissions. A problem here is the possibility of a node having two neighbours (that are not themselves neighbours) transmitting simultaneously, causing a collision only for the node operating in promiscuous mode. Such situations and also the unreliability of the wireless medium makes it very difficult to perform accurate detection.

6. Conclusion

In this paper we have described some of the main protocols for secure routing in mobile ad hoc networks. Most of the preventive protocols provide both authentication, integrity and non-repudiation in addition to increasing the availability of the network services. There are currently no protocols to support confidential exchange of routing information, which will be required for several of the proposed MANET application areas.

Malicious node detection (or intrusion detection) for MANETs rely mainly on detecting protocol deviations by operating the network interface in promiscuous mode. Detection mechanisms must improve its reliability such that confidence can be placed in that malicious nodes are always detected while benign nodes are not.

Acknowledgments

This work has been conducted as part of the EU FP6 OASIS research project, with additional funding by the Norwegian Research Council. Thanks to Ingrid S. Svagård for making this possible.

References

[1] D. Johnson and D. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*. Kluwer Academic Publishers, 1996, pp. 153–181.

[2] C. E. Perkins, E. M. Belding-Royer, and S. Das, *RFC3561: Ad hoc On-Demand Distance Vector (AODV) Routing*. IETF, The Internet Society, Jul. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[3] T. Clausen and P. Jacquet, Eds., *RFC3626: Optimized Link State Routing Protocol (OLSR)*. IETF, The Internet Society, Oct. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[4] IEEE Std. 802.11:2007, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE, New York, USA, Jun. 2007.

[5] L. Zhou and Z. Haas, "Securing ad hoc networks," *Network, IEEE*, vol. 13, no. 6, pp. 24–30, 1999.

[6] D. Johnson, Y. Hu, and D. Maltz, *RFC4728: The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4*. IETF, The Internet Society, Feb. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4728.txt

[7] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," *In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, 1999.

[8] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International*, 2001, pp. 62–68.

[9] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," *Wirel. Netw.*, vol. 11, no. 1-2, pp. 21–38, 2005.

[10] A. Perrig, R. Canetti, D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, pp. 2–13, 2002.

[11] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, 2002, pp. 27–31.

[12] Z. Haas, "A new routing protocol for the reconfigurable wireless networks," in *Proceedings of 6th IEEE International Conference on Universal Personal Communications, IEEE ICUPC'97*, vol. 2. IEEE, New York, USA, Oct. 1997, pp. 562–566.

[13] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the 1st ACM workshop on Wireless security*. Atlanta, GA, USA: ACM, 2002, pp. 1–10.

[14] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated routing for ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 23, pp. 598–610, 2005.

[15] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," in *Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*. IEEE Computer Society, 2003, p. 379.

[16] K. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R. Olsson, "Detecting disruptive routers: a distributed network monitoring approach," *Network, IEEE*, vol. 12, pp. 50–60, 1998.

[17] J. Hughes, T. Aura, and M. Bishop, "Using conservation of flow as a security mechanism in network protocols," in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, 2000, pp. 132–141.

[18] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*. Boston, Massachusetts, United States: ACM, 2000, pp. 255–265.

[19] P. Michiardi and R. Molva, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*. Kluwer, B.V., 2002, pp. 107–121. [Online]. Available: http://portal.acm.org/citation.cfm?id=737297

[20] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confidant protocol," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking \&amp; computing*. Lausanne, Switzerland: ACM, 2002, pp. 226–236.

[21] M. Wang, L. Lamont, P. Mason, and M. Gorlatova, "An effective intrusion detection approach for olsr manet protocol," in *Secure Network Protocols, 2005. (NPSec). 1st IEEE ICNP Workshop on*, 2005, pp. 55–60.

[22] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya, "A game-theoretic intrusion detection model for mobile ad hoc networks," *Computer Communications*, vol. 31, pp. 708–721, Mar. 2008.

[23] N. Marchang and R. Tripathi, "A game theoretical approach for efficient deployment of intrusion detection system in mobile ad hoc networks," in *Advanced Computing and Communications, 2007. ADCOM 2007. International Conference on*, 2007, pp. 460–464.

[24] M. Ramkumar and N. Memon, "An efficient key predistribution scheme for ad hoc network security," *Selected Areas in Communications, IEEE Journal on*, vol. 23, no. 3, pp. 611–621, 2005.

[25] N. Saxena, G. Tsudik, and J. H. Yi, "Threshold cryptography in p2p and manets: The case of access control," *Computer Networks*, vol. 51, no. 12, pp. 3632–3649, Aug 2007.