Wireless networking security: open issues in trust, management, interoperation and measurement

Joseph B. Evans,* Weichao Wang and Benjamin J. Ewy

Department of Electrical Engineering and Computer Science,
University of Kansas,
Lawrence, KS 66045-7621, USA
E-mail: evans@ku.edu E-mail: weichaow@eecs.ku.edu
E-mail: bewy@eecs.ku.edu
*Corresponding author

Abstract: The pervasive availability and wide usage of wireless networks with different kinds of topologies, techniques and protocol suites have brought with them a need to improve security mechanisms. The design, development and evaluation of security techniques must begin with a thorough analysis of the requirements and a deeper understanding of the approaches that are practical within the system constraints. In this paper, we investigate the recent advances in wireless security from theoretical foundations to evaluation techniques, from network level management to end user trust inference and from individual protocol to hybrid systems. We identify the open security issues associated with trust, management, interoperation and measurement. These problems, whose solutions are different in nature and scale from their companions in wired networks, must be properly addressed to establish confidence in the security of wireless networking environments.

Keywords: wireless network security; trust; management; interoperation; measurement.

Reference to this paper should be made as follows: Evans, J.B., Wang, W. and Ewy, B.J. (2006) ‘Wireless networking security: open issues in trust, management, interoperation and measurement’, *Int. J. Security and Networks*, Vol. 1, Nos. 1/2, pp.84–94.

Biographical notes: Joseph B. Evans is the Deane E. Ackers Distinguished Professor of Electrical Engineering and Computer Science and Director of Research Information Technology at the University of Kansas. He recently served as a Program Director in the Division of Computer and Network Systems in the Directorate for Computer and Information Science and Engineering at the National Science Foundation. His research interests include mobile and wireless networking, pervasive computing systems, high speed networks and adaptive computing systems. He has been involved in major national high performance networking testbeds and broadband wireless mobile networking efforts, and has published over 100 journal and conference works. He received a PhD from Princeton University in 1989, is a senior member of the IEEE and a member of the ACM.

Weichao Wang is an Assistant Professor in the Department of Electrical Engineering and Computer Science at the University of Kansas. He is also an active researcher in the Information and Telecommunication Technology Center (ITTC) at the University of Kansas. He received a bachelor degree in Computer Science from Tsinghua University, China in 1998, and a PhD in Computer Science from Purdue University in 2005. His research interests include designing protocols and mechanisms to secure pervasive systems, especially the resource-restraint wireless networks. The investigation focuses on integrating multi-disciplinary schemes with network techniques to prevent and detect various attacks and to enforce security and privacy in such environments. Currently, he is a member of IEEE and ASEE.

Benjamin J. Ewy is a PhD candidate in the Department of Electrical Engineering and Computer Science at the University of Kansas. He is actively researching probabilistic solutions to network security and network management problems, and has served as lead investigator on federally funded research on coordinating pervasive wireless devices. He has more than 10 years of professional engineering experience providing network security and network management analysis, design and implementation for telecommunication carriers, ISPs and enterprises. He is a senior member of the IEEE, a member of USENIX, a member of the ACM, and received the BSCoE and MSEE from the University of Kansas in 1992 and 1995, respectively.

Copyright © 2006 Inderscience Enterprises Ltd.

1 Introduction

The growth in the variety and usage of wireless networks has greatly increased the urgency to identify security approaches. In this paper, we explore recent advances in wireless security and identify open security issues associated with trust, management, interoperation and measurement. These problems, whose solutions are different in nature and scale from their companions in wired networks, must be solved in order to fully exploit the potential of wireless networking. This will enable further growth and investment in wireless networking technology and applications.

The topics we discuss in this paper are critical to creating secure and trustworthy wireless networks. They are interrelated and build upon one another. Establishing and understanding trust relationships is the foundation for implementing security, and is the basis for many of the other issues on which we focus. Management of security relationships and their attendant information is a requirement for any practical wireless networking implementation. Integration builds upon effective trust relationships and management schemes and involves overcoming issues of heterogeneity and interoperation that are becoming increasingly prevalent in wireless networks that utilize technologies spanning the range from telephony to the internet. Evaluation, metrics, and measurement are necessary to establish and deploy credible solutions in wireless network security.

Wireless network architecture determines the relevance and importance of the issues and the range of possible approaches to securing these networks. We consider issues for architectures including mobile ad hoc networks, public access networks such as hotspot and mesh networks, and sensor networks.

This paper is organised as follows: in Section 2, we discuss issues relating to trust, in Section 3, we investigate security management, in Section 4, we review security interoperation in heterogeneous wireless networks, in Section 5 we briefly discuss measurement and evaluation and we conclude in Section 6, with a reprise of the most pressing open issues.

2 Trust management in wireless networks

Trust is an important factor in security that describes a set of relations among the entities engaged in various protocols. These relations are established based on a body of assurance evidence and have been used to mitigate various malicious attacks (Lamsal, 2001). Although many research efforts have studied the establishment and maintenance of trust in complex systems with fixed infrastructure such as the Internet, the existing approaches to trust establishment usually require a lengthy process and assume long term validation. In contrast, few of these characteristics are prevalent in wireless networks with their unreliable transmission medium, frequent topology changes and variable network lifetimes. Therefore, trust management in wireless networks remains a challenging problem and requires considerable attention. If there are highly trustworthy nodes in the wireless network (e.g. base stations in cellular systems or access points in WLAN), many existing approaches to trust formation can be directly applied with minor changes. Therefore, in this section we focus on trust establishment in self-organised environments such as ad hoc networks.

As discussed by Eschenauer et al. (2002), trust establishment in mobile ad hoc networks has three special features:

1 the procedure must be accomplished in a distributed manner without the help from a pre-established trust infrastructure

2 the trust relations are usually short-lived and online-only and

3 the relations are formed based on incomplete evidence.

When a group of wireless nodes form an ad hoc network and start to interact with each other, any pair of nodes that plan to communicate securely must establish a certain level of trust between them in a rapid manner. Mechanisms must be designed to locate a path through which the relationship can be established based on the limited amount of information that every node holds for other members.

The trust value that a node ascribes to another member in the network can be updated based on direct interaction experiences or recommendations from a third party. Since in an ad hoc network every node only has a partial view of the global environment, mechanisms must be designed to enable the mobile nodes to collect and identify the valid evidence and prevent the attackers from manipulating the trust values of other members.

Once the trust values of the mobile nodes are determined, they must be properly and seamlessly integrated into various security mechanisms to enforce information confidentiality, data integrity, user privacy and network performance. The integration may complicate the behaviour of the protocols. For example, route updates might be caused by trust value changes. Therefore, new mechanisms must be designed to investigate the impact of trust on the stability and performance of the networks.

2.1 Trust formation

Trust formation targets the problem of bootstrapping trust between strangers to enable secure communication and authentication in ad hoc networks. It usually involves a procedure to locate a certificate for the communication peer or determine an encryption key. For example, in Balfanz et al. (2002), to enable two mobile devices that have never interacted with each other before to communicate securely, the authors propose a pre-authentication mechanism over a location-limited channel. The small propagation range of the signals on the channel limits the ability of a malicious node to mount passive attacks to subvert the exchange. Since only the commitments of the security keys need to be exchanged, the channel can have a very low data rate.

Since it may be unpractical to assume that a location-limited channel exists between every pair of nodes in a large-scale ad hoc network, researchers have adopted mechanisms very similar to PGP (Garfinkel, 1994) to initiate the trust formation. In Capkun et al. (2003), every node issues certificates to other members that it trusts based on previous experiences. When a node *u* wants to authenticate the public key K_v of another node *v*, the two nodes combine their certificate repositories to locate a certificate chain. Due to the small world phenomenon, the nodes can authenticate each other through a chain with an acceptable length.

Ren et al. (2004) argue that the procedure of self-issuing certificates can be both complex and slow. Their approach, therefore, is to introduce a secret dealer into the network during the initiation phase and allow the dealer to inject a short list of certificates to every node. Through adjusting the length of the list and the choices of the certificates, the proposed mechanism achieves a shorter authentication chain compared to Capkun et al. (2003). It also demonstrates good scalability and high efficiency under dynamic member changes.

To investigate the stability of the trust establishment procedure, the researchers have modelled the ad hoc network as an undirected graph based on preexisting trust relations and cast the trust computation problem as a cooperative game (Baras and Jiang, 2004). The proposed mechanism adopts a localised voting method and both the analysis and simulation results show a phase transition phenomenon: when the probability that a trust relation exists between any pair of nodes exceeds a threshold, the probability that at least one secure path exists between a pair of nodes becomes significantly greater than zero. This result helps answer the fundamental question of the number of pre-existing trust relations that are required to form a generally mutual-trusted community.

In Jiang and Baras (2004), the researchers propose an approach to trust certificate distribution based on the swarm intelligence paradigm. Every node, when it looks for a specific certificate, will leave some 'track' along the path allowing the intermediate nodes to learn the locating route and result. The accumulated information will guide the later nodes to locate the optimal paths towards their targets. This approach is particularly suitable for dynamic environments.

2.2 Trust evolution

The trust value that a node holds against another node can be updated based on direct interaction experiences between them or a recommendation from a third party (Eschenauer et al., 2002). The former factor is usually more reliable. However, trust updates solely based on direct interactions can be very slow. On the other hand, it may be dangerous to allow anyone to make recommendations within the ad hoc network. To prevent the malicious nodes from manipulating the trust values of the innocent members, mechanisms must be designed to guide the evolution procedure.

In Theodorakopoulos and Baras (2004), the ad hoc network is modelled as a weighted, directed graph: the vertices represent the nodes, and the edges represent the trust relations. Every relation contains two values: the *trust* value to estimate the trustworthiness and the *confidence* value to describe the accuracy of the assignment. The authors define two operators that can combine the trust relations along a path or across different paths, respectively. These two operators, together with the graph, form a semiring within which the mechanism can calculate the trust-confidence value between any pair of nodes or determine the most trustworthy path between them.

Different from Theodorakopoulos and Baras (2004) in which only local observations are used to derive the trust values, Buchegger and Le Boudec (2004) considers both first hand experiences and recommendations. Every node maintains a *reputation rating* and a *trust rating* about everyone else, which represent predictions of the other node's behaviour and its capability to make good recommendations, respectively. A modified Bayesian approach is adopted for the updates to the ratings, which prevents the values from fluctuating rapidly. While the estimates of the experiences and recommendations will deteriorate as time passes, the mechanism focuses on the latest performance of a node. While the approach prevents any sudden changes to the trust values, one potential attack that the malicious nodes can conduct is to gradually destroy the reputation of the innocent members by slowly decreasing the ratings in their recommendations.

To investigate the dynamic evolution of trust in an ad hoc network, researchers have cast the convergence behaviour as an algebraic graph problem (Jiang and Baras, 2005). Similar to Theodorakopoulos and Baras (2004), the network is modelled as a directed graph and every trust relation is represented by a trust value and a confidence value. A weighted voting method is designed through which the trust values of the nodes are updated based on feedback from their neighbours. The method treats time as discrete slots and transforms the trust evolution problem to matrix multiplication operations. One factor that may impact the accuracy of this model is the assumption of a constant confidence value, which will seldom happen in practical situations.

The approach Zouridaki et al. (2005) combines the advantages of Buchegger and Le Boudec (2004) and Theodorakopoulos and Baras (2004). It also adopts a Bayesian approach to calculate the trust values, which are assumed to follow a beta distribution. A contribution of this approach is that it combines trust and confidence metrics and derives a new value called 'trustworthiness', which can be integrated into various security protocols such as routing mechanisms.

To reduce the overhead caused by the dissemination of the recommendations, an evidence exchange method is proposed in Capra (2004). Whenever a direct interaction happens between two nodes, they will issue an evaluation for each other. This procedure will enable every node to collect a group of references from other members in the network. These references can be used as recommendations when the trust value of the node is updated later. To prevent the malicious nodes from selectively preserving only the ‘good’ references, every evaluation is protected by a digital signature and a time stamp.

2.3 *Trust-based applications*

As we have discussed earlier in this section, trust can be integrated into various protocols to improve the security of wireless networks. Below we illustrate examples in routing, data management and access control.

Secure routing protocols for ad hoc networks often depend on encryption mechanisms to protect the routing information. A potential improvement, as described by Nekkanti and Lee (2004), is to adapt the encryption methods to the security conditions in the network. The authors propose to link the strength of the encryption algorithm (e.g. key length) to the trustworthiness of the intermediate nodes so that the processing overhead during the route discovery and maintenance procedure will be reduced. The approach also adopts a mechanism similar to Kong and Hong (2003) to preserve the anonymity of the source node.

In Virendra and Upadhyaya (2004) the authors propose to divide the mobile nodes into different domains based on their trust values and interests. The nodes belonging to the same domain monitor each other’s behaviour and when a malicious attacker is located, secure polling will be conducted to exclude the member. To achieve fairness as well as balance the power consumption at different nodes, a domain head election algorithm is executed periodically so that the responsibility and overhead will rotate amongst the domain members.

The research efforts in Gray et al. (2002) target establishing a trust-based admission control mechanism in collaborative ad hoc applications. When a new member attempts to join a collaborative application, every current member has to cast a vote based on the credentials presented by the requestor and the local trust-based policies. The trust formation procedure is integrated into the admission control method to manage the interactions between previously unknown users.

2.4 *Suggested research directions*

Although some advances have been made in trust management in ad hoc networks, several problems remain under-explored and may impede the further development of innovative approaches.

A problem that impacts the accuracy of trust value updates is the validation of second-hand experiences, for example, the recommendations. Some pioneering research is discussed in Marti et al. (2000), which establishes watchdog and pathrater components to monitor the behaviour of neighbours. A more generic approach is required to monitor other portions of the behaviour of any node and collect evidence to assess its trust value. The research challenges include determining the percentage of activities to be monitored, designing efficient methods for storage and dissemination, and evidence-at-the-tip query methods.

The behaviour of a mobile node and the accuracy of the recommendations that it makes are closely related to the application context. Few trust management approaches in wireless networks have addressed this factor. One reason is that researchers typically derive a trust value that can be applied to particular target environments. The next step in trust research is to identify the context-related features and the context-independent features and use the results to develop context-aware trust management mechanisms.

Most of the current trust management approaches focus on the establishment and maintenance of trust relations among nodes or users in the network. With the ever-increasing popularity of data-intensive applications, trust might be interwoven into the data transferred on the network. This would drastically reduce the overhead to establish, update and maintain trust relations among the entities in wireless networks without deteriorating the integrity and quality of the information.

3 Managing security in wireless networks

The requirements of a particular operating environment place many demands on the ability to manage an overall security solution. Often trade-offs between ease of use, policies capturing the desired level of security and the technical limitations must be explored. We investigate two rapidly evolving operating environments, public access networks and sensor networks and discuss the issues in how they manage authentication and access control, session (mobility), resources and accounting (billing).

3.1 *Public access networks*

The proliferation of 802.11-based hotspots and their ad hoc extension as meshes has created a demand for the ability to securely mutually authenticate the access point and the mobile user. IEEE 802.1X (IEEE Std 802-1x, 2001) defines a mechanism for authenticating the client and access point, and controlling access to the wireless ‘port’. It requires a pre-shared secret between the user and network, and as such is most appropriate in the enterprise environment.

Public access hotspots often have business models that need to support single use authorisation such as prepaid cards, as well as allow an access point and its corresponding scarce RF spectrum to be utilised by more than one service provider. Typically these public access hotspots utilise a web-based front-end to an authentication system that performs packet filtering on some combination of the MAC and IP address, or proprietary client software that reduces interoperability options. Because of the ease of spoofing both the MAC and IP addresses it is possible to deny legitimate users access to the network, or use their credentials for unauthorised access to the network. Systems have been designed that allow clients to pick from different service providers by utilising Remote Authentication Dial In User Service (RADIUS) (Rigney et al., 1997) messages to authenticate with their preferred provider (Anton et al., 2003), but must address not only mutually authenticating the client and access point, but also the various service providers.

Matsunaga et al. (2003) detail a solution for the confederation of service providers that allows a customer to select both the authentication method and service provider, while preventing the exposure of private information to the local access point infrastructure. The approach utilises a preexisting certificate authority infrastructure, and assumes trust relationships between the user and the service provider, and the service provider and the access point. This single sign-on system architecture supports multiple authentication methods including a RADIUS approach, and includes a policy engine to manage access control. It includes a mechanism for allowing encryption in the public access scenario without pre-shared keys using 802.1X guest privileges, and incorporates the session key into a compound authentication step with the web-based login.

Community-based meshes extend the public access point by providing multi-hop connectivity to extend the systems range. Community meshes for public access typically have access to infrastructure for authentication and access control, and as such are able to take advantage of the same techniques as used in hotspot architectures. Resource management is much more important in a mesh network, and work in the area of resource management, including in the areas of topology control via power management (Li et al., 2001) and improving spatial reuse by utilising a time-slotted transmission scheduling to maximise fair use (Hubaux and Ben Salem, 2005; Liu et al., 2001), has demonstrated the ability to alleviate resource problems. There is need for continued research (Akyildiz et al., 2005) particularly in understanding the trade-off in power management for mobile stations participating in the mesh while simultaneously maximising connectivity.

A number of investigations into methods for encouraging and rewarding participation in the mesh routing to improve connectivity have been performed. In Ben Salem et al. (2003), the authors designed a system that utilises accounting to track the efforts done on behalf of other nodes for the purpose of rebates or settlements. This system is based on symmetric keys to create and track end-to-end sessions. Jakobsson et al. (2003) present a lightweight micro-payment scheme that utilises an accounting base and heuristics to minimise fraud while providing incentives to forward other's data. Additional work to develop systems that do not require end to end coordination, as well as more exact metrics, will be needed before the risks of fraud are reduced to allow financial incentives for a more ad hoc deployment of meshes.

Managing session level roaming in public access networks requires mechanisms beyond layer two, but if there is going to be encryption and authentication at layer two, it needs to support roaming, and provide hooks for initiating the roam. Depending on the implementation, roaming decisions may be made by the mobile terminal, and this requires a mechanism for transitioning any session keys such as the pairwise master key in IEEE 802.11i (IEEE Std 802-11i, 2004) from one access point to another. Upper layer solutions have been explored by some, including relying on IPSEC for authentication and encryption (Zhang et al., 2002a), and others that utilise Mobile IP (Ramjee et al., 2000; Barton et al., 2002), multi-layer approaches (Kong et al., 2002b; Matsunaga et al., 2003; Zan et al., 2005), and overlay-based approaches (Zhuang et al., 2003). The trade-offs in complexity of implementation and deployment, features provided, and the communication overhead and inefficiencies, leave many areas to be explored.

3.2 Sensor networks

Sensor networks present a dramatically different operating environment to public access wireless networks. Some of the key differences include lack of connectivity to public infrastructure, the nature of the traffic flow, and node limitations in the areas of processing, power availability and memory.

Managing authentication is directly impacted by the lack of connectivity; the nodes cannot rely on a key server infrastructure in many deployment scenarios. Node limitations also restrict the cryptographic primitives available, typically the nodes do not have processing resources (Hill et al., 2000; Kahn et al., 2000) to perform public key encryption methods or memory to store keys, reducing the strength of algorithms and placing limits on deployment sizes.

Key distribution in the absence of a central key server infrastructure has been the focus of much research. A popular approach is to utilise a probabilistic predistribution of keys (Du et al., 2003; Eschenauer and Gligor, 2002; Liu and Ning, 2003), the basic idea of which is to preload each node with a set of keys, such that a node has some percentage chance of being able to have a common key with neighbour nodes when it is deployed. Chan et al. (2003) present three different options for performing the predistribution, with trade-offs to improve small attack survivability, improved reliability against node compromise and the ability to perform mutual authentication. Zhu et al. (2003) utilise a deterministic algorithm to select the subset of keys being assigned to a node based on a node identifier. This allows neighbour nodes to determine key overlap without communicating identifiers for each known key; they only have to share their own node identifier.

Traffic flow in sensor networks is, in many cases, from each sensor to a central collector station, often over multiple hops. Aggregation and duplicate elimination (Madden et al., 2002) is desirable to reduce bandwidth consumption and save power. In order for intermediate hops to be able to perform these services, the authentication and encryption need to be link-based (Karlof et al., 2004; Perrig et al., 2001) instead of end-to-end (Dierks and Allen, 1999; Kent and Atkinson, 1998).

Bohge and Trappe (2003) pursue an alternate direction for handling node limitations with the extension of TESLA (Perrig et al., 2000) to create small symmetric key certificates, and impose a hierarchy to the sensor nodes, such that more capable forwarding nodes handle all communication between sensor nodes and the access point. Sensor nodes do not forward packets for each other, and therefore only need to authenticate with the closest forwarding node. This topological constraint comes with a corresponding loss of flexibility in deployment of the sensor nodes.

Continuing challenges for the management of sensor networks include improved key distribution schemes, detection of and protection from compromised nodes, and continued development of support for elliptic public-key schemes (Malan et al., 2004). Perrig et al. (2004) established that increased packet transmission latencies due to security information overhead are much larger than the corresponding computation time, and asserted that future gains will likely come from careful design and implementation of security protocols, as opposed to dedicated cryptographic hardware.

4 Heterogeneity and security in wireless networks

The recent years have witnessed the rapid development of wireless networking technologies and an increasing heterogeneity in protocol suites, portable devices and innovative applications. Combinations of different techniques have been adopted to provide transparent, pervasive network access to the users. For example, mobile ad hoc networks have been used to extend the coverage and improve the bandwidth usage of cellular systems (Bhargava et al., 2004; Lin and Hsu, 2000; Luo et al., 2003; Wu et al., 2001). Internet-based mobile ad hoc networks take advantage of the fixed infrastructure to provide ubiquitous communication services to users (Corson et al., 1999; Lim et al., 2006); and 3G/WLAN integration provides both high speed data transmission and wide coverage (Wang et al., 2005).

Although this diversity enables users to access network resources ubiquitously, it generates new challenges in enforcing security and preserving privacy in such heterogeneous systems. The differences in processing capabilities and available bandwidth, supported encryption mechanisms and adopted trustworthiness propagation methods introduce new vulnerabilities that cannot be overcome by current approaches. The security challenges driven by heterogeneous environments have attracted many researchers and some pioneering work has been conducted (Bharghavan, 1997; Lamparter and Westhoff, 2002; Naqvi and Riguidel, 2004; Schwiderski-Grosche et al., 2004; Sterbenz et al., 2002). Integrating these concepts and prior research results, we divide the research problems in securing heterogeneous wireless networks into the following four subcategories, enabling authentication, developing incentives for collaboration, preserving service availability and reliability and preserving data privacy.

In a heterogeneous system, the users can dynamically switch among different networks. This may be caused by node movement or the intent to improve the connection quality. At the same time, the data traffic between mobile nodes belonging to different networks may be transferred by several different techniques before reaching the eventual destinations. Therefore, a generic authentication architecture must be developed to support flexible and efficient validation of user identities, and to prevent fraudulent data transmissions.

Under many conditions, the heterogeneous system contains a self-organised network such as a Mobile Ad hoc Networks (MANET), in which the users are rational and suitable incentives must be provided to encourage the mobile nodes to store and forward data for other users. The heterogeneity causes new challenges in verifying the identities of the intermediate nodes and crediting and redeeming the incentives.

The differences in available resources in different networks (e.g. bandwidth) can be used to conduct DOS attacks. To prevent the networks with weaker processing capabilities or less bandwidth from being overwhelmed, new mechanisms must be developed to balance the internetwork workload.

It is more difficult to establish and maintain trust relationships among mobile nodes in different networks. Therefore, when data is transferred across multiple networks, new approaches must be designed to protect user privacy and weave trust into the data traffic.

4.1 Authentication in heterogeneous networks

Based on whether one or multiple predetermined authentication centres are required in the heterogeneous network, the existing approaches can be divided into two groups: centralised mechanisms and self-organised mechanisms.

The centralised mechanisms usually select some special nodes in the network that are more difficult to compromise or have higher trustworthiness to serve as the authentication centres. For example, in a heterogeneous multi-layer ad hoc network (Kong et al., 2002a) that contains ground mobile nodes, ground backbone nodes and unmanned aerial vehicles (UAVs), since the UAVs are the most difficult to capture and compromise, they play the roles of Certification Authorities (CA) and provide the authentication services. Every mobile node has a personal RSA key pair in which the public key is certified by the CA. To support the revocation when a compromised node is detected, the CA will generate and flood the Certificate Revocation List (CRL) across the network. When two mobile nodes want to initiate secure communication, they authenticate each other by verifying the certificates and examining the authentic up-to-date CRLs. Similar approaches have been adopted by the heterogeneous networks that integrate MANET and cellular systems (Bhargava et al., 2004) or Wireless LAN and cellular systems (Shi et al., 2004), in which the base stations and home agents will provide the authentication services respectively.

Asymmetric encryption provides strong security when the mobile nodes authenticate each other's identity. However, because of its heavy computation overhead, it is very difficult to apply to packet level authentication. Researchers have adopted a message authentication code (MAC) approach to accomplish this task. In Luo et al. (2003); Ben Salem et al. (2003), a keyed hash function is used to protect the integrity of the data packets and authenticate the relay paths. Since every intermediate node only needs to conduct one hash function based on the received packet and the previous MAC value, very little computation overhead is incurred when the relaying procedure is chained.

A special feature of wireless networks is their highly dynamic membership and topology. Therefore, authentication architectures based on Static Security Associations (SSA) do not satisfy the security requirements in these systems. To compensate for this disadvantage, researchers have proposed flexible SAs (FSAs) (Wang et al., 2005) that are created on demand to provide temporary security services. This scheme can drastically reduce the number of SAs among wireless networks, which has been identified as an important factor for security and manageability (Aboba and Vollbrecht, 1999).

Centralised authentication mechanisms, although improved through various techniques, still suffer from single-point of service denial. To compensate for this disadvantage, researchers have developed infrastructureless or self-organised approaches. Based on secret sharing (Shamir, 1979), the solution in Kong et al. (2002a) distributes the functionality of a certification authority among the wireless nodes. Each node holds a partial secret key, and K-out-of-N nodes can generate a legitimate certificate. A similar idea has been adopted by Yang and Lu (2002), in which the interval to renew the certificate doubles every time for a well-behaved wireless node so that the overhead caused by these operations becomes lower and lower as time evolves.

4.2 Incentive for collaboration

Under many conditions, the heterogeneous wireless networks will contain a self-organised environment like a MANET. Since relaying packets for other users will consume the battery power and bandwidth resource of the intermediate nodes, it is natural to assume that these nodes are rational and need some incentives for offering services. Both reputation-based (Buchegger and Le Boudec, 2002; Michiardi and Molva, 2002) and reward-based approaches (Buttyan and Hubaux, 2000, 2003; Zhong et al., 2003) for pure ad hoc networks have been proposed and investigated. These mechanisms have also been extended to heterogeneous networks.

The research challenges for designing incentives, as summarised in Ben Salem et al. (2003), are to enforce payment by the users enjoying the forwarding services, and prevent dishonest reward claims and free packet riding. In Lamparter et al. (2003), the researchers investigate cooperation in the internet-based ad hoc networks and adopt an Internet Service Provider to authenticate the intermediate nodes using asymmetric encryption. In Luo et al. (2003), a solution is described that depends on piggybacked MAC codes to authenticate the relay path in multi-hop cellular networks. The source node and every intermediate node along the path to the base station will calculate a keyed hash result that covers the data packet, the previous MAC value, and the neighbours' identities so that no single attacker can remove or add nodes to the path.

The efforts by Ben Salem et al. (2003) improve the reward mechanism in multi-hop cellular networks by integrating MAC codes with stream ciphers. Every intermediate node will encrypt the data packet by XORing it with a stream cipher that is determined by the node's secret key and the session identifier of the data traffic. Through this mechanism, no node can be inserted into or removed from the relay path since the extra stream cipher will prevent the destination from recovering the original information. It also prevents free riding. The mechanism separates payment from the confirmation of the reception, which prevents refusal to pay.

In Maille (2005), the researchers adopt an economic analysis to answer two questions in multi-hop cellular networks:

1 What discount should be offered to the users that agree to relay packets for other nodes?

2 Does offering such an option improve the net benefit of the service provider?

Their approach is based on a simplified model: the users choose whether to agree to relay packets for other nodes when they join the network, and the choice will lead to different charging prices. Using the leader-follower game model, the analysis shows that allowing multi-hop relaying in cellular networks can work to the benefit of the service provider in dense networks since the savings in installation and maintenance exceed the loss in revenue caused by fee discounts.

4.3 Prevention of DOS attacks

When heterogeneous wireless techniques are integrated, the networks with higher bandwidth or higher processing power can overwhelm the networks with fewer resources by injecting a large amount of traffic or a large number of authentication requests, thus conducting DOS attacks. To defend against such attacks, new mechanisms must be designed to prevent the overload from occurring. We review two groups of defensive approaches.

The first group of approaches focuses on prevention mechanisms. For example, (Enck et al., 2005) the authors explore the vulnerabilities in cellular networks supporting a Short Messaging Service (SMS). In current cellular systems, both voice and SMS traffic use the same control channels for session establishment. Since many cellular service providers now allow the users to send short messages through high-speed internet, malicious users can send a large number of messages in a short time to saturate these channels, thus paralysing voice service in a given area. To defend against such attacks, the authors suggest adopting various methods to limit the rate that short messages can be introduced into the network. Although practical as a short-term approach, this method will face two problems when it is generalised to other environments. Firstly, rate limitation requires a global, real-time vision of bandwidth utilisation as well as congestion prediction in the network, which cannot be easily achieved in heterogeneous wireless systems, especially when self-organised networks are involved. Secondly, rate limitations may decrease network resource utilisation, which conflicts with the service provider's interests. How to balance these requirements remains an open question and deserves further research attention.

The second group of approaches focuses on helping the networks with fewer resources to improve their utilisation. For example, in 3G wireless data networks, the multicast data rate is determined by the lowest value of all the receivers, which may significantly impact the bandwidth utilisation. To increase the multicast throughput, researchers have proposed Integrated Cellular and Ad Hoc Multicast (ICAM) (Bhatia et al., 2006). The multicast group member with a low data rate will ask a proxy with a better channel quality to relay packets for it. The analysis shows that optimal ICAM is NP-hard, and a bounded, polynomial-time algorithm was developed to construct the multicast forest.

The approach by Loa and Cui (2005) considers more complicated scenarios when multiple multicast groups are present in the network. To maximise the utilisation of the ad hoc network, the base station must choose a subset of groups and keep them in the cellular systems. The authors formulate the problem to a multidimensional knapsack problem, and then propose a dynamic algorithm with polynomial-time complexity.

4.4 *Suggested research directions*

Although significant research efforts have been directed at securing heterogeneous wireless networks, several fundamental questions remain under-explored.

Many of the existing approaches to improving security in heterogeneous wireless networks are conducted in an ad hoc fashion - the researchers choose a heterogeneous scenario, identify a specific vulnerability and design a prevention mechanism. This approach, although practical in the short term, will not scale with the increasing diversity of network techniques and applications. An important research direction, therefore, is to develop a *generic security management protocol* that can be understood by all techniques. With this protocol, different networks can identify the security requirements and supported security primitives. When an end-to-end transmission path penetrating multiple networks is established, this protocol will enable the mobile users to locate the most vulnerable component on the path and guide the choice of route and encryption operations. Only when heterogeneous wireless networks speak the same 'language' and exchange the appropriate information can generic and scalable security mechanisms be efficiently deployed.

To defend against DOS attacks introduced by foreign networks, the local network must be able to monitor the resource usage efficiently and make adjustments properly. The design of such a mechanism may require the users to derive a global vision of the network based on localised observations. The incurred computation and communication overhead must be carefully planed to avoid impact on network performance.

In heterogeneous wireless systems, the malicious nodes can collude not only within the local network, but also crossing multiple networks. Therefore, new mechanisms must be designed to prevent the attackers in different networks from jointly compromising the infrastructure. This problem is especially challenging when self-organised environments are involved.

When the data traffic in an end-to-end transmission passes multiple networks, different security and privacy protection mechanisms might be adopted. The differences among these mechanisms can impact the confidentiality and privacy of the data. New approaches must be designed to evaluate the compatibility of these mechanisms and identify appropriate combinations to enforce security.

These research challenges, if addressed, can contribute to answering the fundamental questions in understanding the security in heterogeneous wireless networks, and provide guidelines for the design of innovative approaches.

5 Measurement and evaluation of wireless network security

With the evolution of ideas and systems, it is important to establish criteria for evaluating the variety of routing and authentication methodologies to provide insight into trade-offs that implementation will require.

One of the most fundamental measures of a particular security solution in the wireless environment is the impact of that approach on the resources required to handle mobile node handoff, both within an Autonomous System (AS) and between them. Zhang et al. (2002b) have compared four different inter-AS rekeying protocols in a hierarchical key distribution environment. They study a range of mobility scenarios, and compare message rates and number of keys to be stored, and find the algorithms that excel under different trade-offs. Additional comparisons and measurements of alternate deployment scenarios and technologies will greatly improve our understandings of the trade-offs involved.

Camtepe and Yener (2005) provide a detailed taxonomy of wireless sensor network key distribution methods, and evaluate the methods under a variety of different metrics. Their taxonomy decomposed the problem space into hierarchical and distributed sensor networks, and within each of those two classes found examples of pair-wise, group-wise and network-wise key distribution. They provide a detailed comparative analysis of the reviewed solutions with respect to scalability, key connectivity, resilience, storage complexity, processing complexity and communication complexity, and conclude that there are significant trade-offs between existing solutions. More evaluations of this type provide excellent feedback for researchers to expand and improve algorithms under development.

Kambourakis et al. (2004) evaluate an end-to-end authentication solution using public key infrastructure in the public access network environment. They propose an authentication protocol, and assess it in terms of network response time, request preparation time, total handshake time, total call set-up, memory utilisation and power consumption. They develop a testbed environment and evaluate their protocol, providing a valuable framework to perform future comparative evaluations.

Karlof and Wagner (2003) review a number of wireless routing protocols, including discussions of the types of attacks possible, but there has been little attention to metrics for the comparative analysis and measurement of security attributes for these protocols. This is a promising and important area for future work.

6 Conclusion

In this paper, we have reviewed wireless network security issues in trust, management, interoperation and measurement and have identified a number of open problems in these areas.

Open issues in trust include

1 developing efficient evidence collection mechanisms to support techniques that infer trust

2 constructing context-aware trust assessment schemes and

3 understanding and implementing techniques for embedding trust information into data.

Critical issues in management of security relationships in public access networks include

1 multi-provider authentication

2 protection of incentive information and

3 mechanisms to support roaming, and in sensor networks issues such as

4 lightweight key distribution schemes

5 compromised node defense through redundancy and consistency checking and

6 more efficient public-key schemes.

Open problems in secure integration of heterogeneous wireless networks include

1 developing a generic security management protocol that can span the network clouds

2 developing an efficient resource monitoring and planning mechanism and

3 creating techniques to defend against collusive attacks.

Development of metrics, measurements, and evaluation of approaches are important topics urgently requiring further investigation in order to establish a scientific methodology for the entire wireless network security research area.

References

Aboba, B. and Vollbrecht, J. (1999) 'Proxy chaining and policy implementation in roaming', Available at: http://www.ietf.org/rfc/rfc2607.txt. IETF Request for Comments 2607.

Akyildiz, I.F., Wang, X. and Wang, W. (2005) 'Wireless mesh networks: a survey', *Computer Networks Journal (Elsevier)*, Vol. 47, No. 4, pp.445–487.

Anton, B., Bullock, B. and Short, J. (2003) 'Best current practices for Wireless Internet Service Provider (WISP) roaming, version 1.0.', *Wi-Fi Alliance*.

Balfanz, D., Smetters, D., Stewart, P. and Wong, H. (2002) 'Talking to strangers: authentication in ad-hoc wireless networks', *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS)*.

Baras, J. and Jiang, T. (2004) 'Cooperative games, phase transitions on graphs and distributed trust in MANET', *Proceedings of the 43rd IEEE Conference on Decision and Control*, pp.93–98.

Barton, M., Lee, J., Narain, S., Wong, K.D., Atkins, D., Ritcherson, D. and Tepe, K.E. (2002) 'Integration of IP mobility and security for secure wireless communications', *Proceedings of IEEE International Conference on Communications (ICC)*, pp.1045–1049.

Ben Salem, N., Buttyan, L., Hubaux, J-P. and Jakobsson, M. (2003) 'A charging and rewarding scheme for packet forwarding in multi-hop cellular networks', *Proceedings of Forth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp.13–24.

Bhargava, B., Wu, X., Lu, Y. and Wang, W. (2004) 'Integrating hterogeneous wireless technologies: a cellular-assisted mobile ad hoc networks', *Mobile Network and Applications*, Vol. 9, No. 4, pp.393–408.

Bharghavan, V. (1997) 'Challenges and solutions to adaptive computing and seamless mobility over heterogeneous wireless networks', *International Journal on Wireless Personal Communications: Special Issue on Mobile Wireless Networking*. Vol. 4, No. 2, pp.217–256.

Bhatia, R., Li, L.E., Luo, H. and Ramjee, R. (2006) 'ICAM: integrated cellular and ad-hoc multicast', *IEEE Transactions on Mobile Computing*, Vol. 5, No. 8, pp. 1004–1015.

Bohge, M. and Trappe, W. (2003) 'An authentication framework for hierarchical ad hoc sensor networks', *Proceedings of the second ACM Workshop on Wireless Security (WISE'03)*, pp.79–87.

Buchegger, S. and Le Boudec, J-Y. (2002) 'Performance analysis of the CONFIDANT protocol: cooperation of nodes – fairness in distributed ad hoc networks', *Proceedings of the third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*.

Buchegger, S. and Le Boudec, J-Y. (2004) 'A robust reputation system for P2P and mobile ad-hoc networks', *Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems*.

Buttyan, L. and Hubaux, J-P. (2000) 'Enforcing service availability in mobile ad hoc WANs', *Proceedings of the First ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*.

Buttyan, L. and Hubaux, J-P. (2003) 'Stimulating cooperation in self-organizing mobile ad hoc networks', *Mobile Networks and Applications*, Vol. 8, No. 5, pp.579–592.

Camtepe, S. and Yener, B. (2005) 'Key distribution mechanisms for wireless sensor networks: a survey', *Technical Report 05-07*, Department of Computer Science, Rensselaer Polytechnic Institute.

Capkun, S., Buttyan, L. and Hubaux, J-P. (2003) 'Self-organized public-key management for mobile ad hoc networks', *IEEE Transactions on Mobile Computing*, Vol. 2, No. 1, pp.52–64.

Capra, L. (2004) 'Engineering human trust in mobile system collaborations', *Proceedings of the 12th International Symposium on the Foundations of Software Engineering (SIGSOFT)*, pp.107–116.

Chan, H., Perrig, A. and Song, D. (2003) 'Random key predistribution schemes for sensor networks', *Proceedings of the 2003 Symposium on Security and Privacy*, pp.197–215.

Corson, M., Maker, J. and Cernicione, J. (1999) 'Internet-based mobile ad hoc networking', *IEEE Internet Computing*, Vol. 3, No. 4, pp.63–70.

Dierks, T. and Allen, C. (1999) 'The TLS protocol', Available at: http://www.ietf.org/rfc/rfc2246.txt. IETF Request for Comments 2246.

Du, W., Deng, J., Han, Y. and Varshney, P. (2003) 'A pairwise key pre-distribution scheme for wireless sensor networks', *Proceedings of the Tenth ACM Conference on Computer and Communications Security (CCS)*, pp.42–51.

Enck, W., Traynor, P., McDaniel, P. and La Porta, T. (2005) 'Exploiting open functionality in SMS-capable cellular networks', *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS)*, pp.393–404.

Eschenauer, L. Gligor, V. and Baras, J. (2002) 'On trust establishment in mobile ad-hoc networks', *Proceedings of the International Workshop on Security Protocols*.

Eschenauer, L. and Gligor, V. (2002) 'A key-management scheme for distributed sensor networks', *Proceedings of the Ninth ACM Conference on Computer and Communications Security (CCS)*, pp.41–47.

Garfinkel, S. (1994) 'PGP: Pretty Good Privacy', O'Reilly & Associates.

Gray, E., O'Connell, P., Jensen, C., Weber, S., Seigneur, J. and Yong, C. (2002) 'Towards a framework for assessing trust-based admission control in collaborative ad hoc applications', *Technical Report 66*, Department of Computer Science, Trinity College, Dublin.

Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D. and Pister, K. (2000) 'System architecture directions for networked sensors', *Proceedings of Ninth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, pp.93–104.

Hubaux, J-P. and Ben Salem, N. (2005) 'A fair scheduling for wireless mesh networks', *Proceedings of First IEEE Communication Society's Workshop on Wireless Mesh Networks (WiMesh)*.

IEEE Std 802-1x (2001) *IEEE Standard for Local and Metropolitan Area Networks*, *Port-Based Network Access Control*, October.

IEEE Std 802-11i (2004) *IEEE Standard for Wireless LAN Medium Access Control*, *(MAC) and Physical Layer (PHY) Specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements*, June.

Jakobsson, M., Hubaux, J-P. and Buttyan, L. (2003) 'A micropayment scheme encouraging collaboration in multi-hop cellular networks', *Lecture Notes in Computer Science*, Vol. 2742, pp.15–33.

Jiang, T. and Baras, J. (2004) 'Ant-based adaptive trust evidence distribution in MANET', *Proceedings of the 24th International Conference on Distributed Computing Systems Workshops (ICDCSW'04)*, pp.588–593.

Jiang, T. and Baras, J. (2005) 'Autonomous trust establishment', *Proceedings of the Second International Network Optimization Conference*.

Kahn, J., Katz, R. and Pister, K. (2000) 'Emerging challenges: mobile networking for smart dust', *Journal of Communications and Networks*, Vol. 2, No. 3, pp.188–196.

Kambourakis, G., Rouskas, A. and Gritzalis, S. (2004) 'Performance evaluation of public key based authentication in future mobile communication systems', *EURASIP Journal on Wireless Communications and Networking*, Vol. 2004, No. 1, pp.184–197.

Karlof, C. and Wagner, D. (2003) 'Secure routing in wireless sensor networks: attacks and countermeasures', *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp.113–127.

Karlof, C., Sastry, N. and Wagner, D. (2004) 'TinySec: a link layer security architecture for wireless sensor networks', *Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems*, pp.162–175.

Kent, S. and Atkinson, R. (1998) 'Security architecture for the internet protocol', Available at: http://www.ietf.org/rfc/rfc2401.txt IETF Request for Comments 2401.

Kong, J., Luo, H., Xu, K., Lihui Gu, D., Gerla, M. and Lu, S. (2002a) 'Adaptive security for multi-level ad-hoc networks', *Wireless Communications and Mobile Computing*, Vol. 2, No. 5, pp.533–547.

Kong, J., Gerla, M., Prabhu, B.S. and Gadh, R. (2002b) 'Providing multi-layer security support for wireless communications across multiple trusted domains', *Technical Report 020032*, Computer Science Department, UCLA.

Kong J. and Hong, X. (2003) 'ANODR: Anonymous on demand routing protocol with untraceable routes for mobile ad-hoc networks', *Proceedings of the Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*, pp.291–302.

Lamparter, B. and Westhoff, D. (2002) 'Security challenges in the future mobile internet', *Proceedings of the PAMPAS Workshop on Requirements for Mobile Privacy & Security*.

Lamparter, B., Paul, K. and Westhoff, D. (2003) 'Charging support for ad hoc stub networks', *Journal of Computer Communication*, Vol. 26, No. 13, pp.1504–1515.

Lamsal, P. (2001) 'Understanding trust and security', *Department of Computer Science Technical Report*, University of Helsiki, Finland.

Li, L., Halpen, J.Y., Bahl, P., Wangand, Y. and Wattenhofer, R. (2001) 'Analysis of cone-based distributed topology control algorithm for wireless multi-hop networks', *Proceedings of ACM Principles of Distributed Computing Conference (PODC'01)*, pp.264–273.

Lim, S., Lee, W., Cao, G., Das, C. (2006) 'A novel caching scheme for improving internet-based mobile ad hoc networks performance', *Ad Hoc Networks*, Vol. 4, No. 2, pp.225–239.

Lin, Y. and Hsu, Y., (2000) 'Multihop cellular: a new architecture for wireless communications', *Proceedings of IEEE INFOCOM 2000*, pp.1273–1282.

Liu, X., Chong, E. and Shroff, N. (2001) 'Transmission scheduling for efficient wireless utilization', *Proceedings of IEEE INFOCOM 2001*, pp.776–785.

Liu, D. and Ning, P. (2003) 'Establishing pairwise keys in distributed sensor networks', *Proceedings of the Tenth ACM Conference on Computer and Communications Security (CCS)*, pp.52–61.

Loa, L. and Cui, J. (2005) 'Reducing multicast traffic load for cellular networks using ad hoc networks', *Proceedings of the Second International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine).*

Luo, H., Ramjee, R., Sinha, P., Li, L. and Lu, S. (2003) 'UCAN: a unified cellular and ad-hoc network architecture', *Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking (MobiCom).* pp.353–367.

Madden, S., Franklin, M., Hellerstein, J. and Hong, W. (2002) 'TAG: a tiny aggregation service for ad-hoc sensor networks', *Proceedings of the Fifth Symposium on Operating Systems Design and Implementation (OSDI 2002).*

Maille, P. (2005) 'Allowing multi-hops in cellular networks: an economic analysis', *Proceedings of the Eighth ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM).*

Malan, D., Welsh, M. and Smith, M. (2004) 'A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography', *Proceedings of First IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON).*

Marti, S., Giuli, T., Lai, K. and Baker, M. (2000) 'Mitigating routing misbehavior in mobile ad hoc networks', *Proceedings of ACM Mobile Computing and Networking*, pp.255–265.

Matsunaga, Y., Merino, A.S., Suzuki, T. and Katz, R.H. (2003) 'Secure authentication system for public WLAN roaming', *Proceedings of First ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH)*, pp.113–121.

Michiardi, P. and Molva, R. (2002) 'Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks', *Proceedings of the Sixth IFIP Communications and Multimedia Security Conference.*

Naqvi, S. and Riguidel, M., (2004) 'Security architecture for heterogeneous distributed computing systems', *Proceedings of the 38th International Carnahan Conference on Security Technology.*

Nekkanti, R. and Lee, C. (2004) 'Trust based adaptive on demand ad hoc routing protocol', *Proceedings of the ACM Southeast Regional Conference*, pp.88–93.

Perrig, A., Canetti, R., Tygar, J. and Song, D. (2000) 'Efficient authentication and signing of multicast streams over lossy channels', *Proceedings of the 21st IEEE Symposium on Security and Privacy*, pp.56–73.

Perrig, A., Szewczyk, R., Wen, V., Culler, D. and Tygar, J. (2001) 'SPINS: security protocols for sensor networks', *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (MobiCom)*, pp.189–199.

Perrig, A., Stankovic, J. and Wagner, D. (2004) 'Security in wireless sensor networks', *Communications of the ACM*, Vol. 47, No. 6, pp.53–57.

Ramjee, R., La Porta, T., Salgarelli, L., Thuel, S., Varadhan, K. and Li, L. (2000) 'IP-based access network infrastructure for next-generation wireless data networks', *IEEE Personal Communications Systems Magazine*, August 2000, pp.34–41.

Ren, K., Li, T., Wan, Z., Bao, F., Deng, R. and Kim, K. (2004) 'Highly reliable trust establishment scheme in ad-hoc networks', *Computer Networks*, Vol. 45, No. 6, pp.687–699.

Rigney, C., Rubens, A., Simpson, W. and Willens, S. (1997) 'Remote Authentication Dial In User Service (RADIUS)', Available at: http://www.ietf.org/rfc/rfc2138.txt. IETF Request for Comments 2138.

Schwiderski-Grosche, S., Tomlinson, A., Goo, S. and Irvine, J. (2004) 'Security challenges in the personal distributed environment', *Proceedings of the IEEE 60th Vehicular Technology Conference.*

Shamir, A. (1979) 'How to share a secret', *Communications of the ACM*, Vol. 22, No. 11, pp.612–613.

Shi, M., Shen, X. and Mark, J. (2004) 'IEEE802.11 roaming and authentication in wireless LAN/cellular mobile networks', *IEEE Wireless Communications*, Vol. 11, No. 4, pp.66–75.

Sterbenz, J., Krishnan, R., Hain, R., Jackson, A., Levin, D., Ramanathan, R. and Zao, J. (2002) 'Survivable mobile wireless networks: issues, challenges, and research directions', *Proceedings of the First ACM Workshop on Wireless Security (WISE)*, pp.31–40.

Theodorakopoulos, G. and Baras, J. (2004) 'Trust evaluation in ad-hoc networks', *Proceedings of the ACM workshop on Wireless security*, pp.1–10.

Virendra, M. and Upadhyaya, S. (2004) 'Securing information through trust management in wireless networks', *Proceedings of the Workshop on Secure Knowledge Management (SKM)*, pp.201–206.

Wang, W., Liang, W. and Agarwal, A. (2005) 'Integration of authentication and mobility management in third generation and WLAN data networks', *Journal of Wireless Communications and Mobile Computing,* Vol. 5, No. 6, pp.665–678.

Wu, H., Qiao, C., De, S. and Tonguz, O. (2001) 'Integrated cellular and ad hoc relaying systems: iCAR', *IEEE Journal on Selected Areas in Communications*, Vol. 19, No. 10, pp.2105–2115.

Yang, H. and Lu, S. (2002) 'Self-organized network layer security in mobile ad hoc networks', *Proceedings of the First ACM Workshop on Wireless Security (WISE)*, pp.11–20.

Zan, L., Wang, J. and Bao, L. (2005) 'Personal protocol for mobility management in IEEE 802.11 systems', *Proceedings of Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MOBIQUITOUS).*

Zhang, J., Li, S., Weinstein, N. and Tu, N. (2002a) 'Virtual operator based AAA in wireless LAN hot spots with ad-hoc networking support', *ACM Mobile Computing and Communications Review*, Vol. 6, No. 3, pp.10–21.

Zhang, C., DeCleene, B., Kurose, J. and Towsley, D. (2002b) 'Comparison of inter-area rekeying algorithms for secure wireless group communications', *Performance Evaluation*, Vol. 49, Nos. 1–4, pp.1–20.

Zhong, S., Yang, Y. and Chen. J. (2003) 'Sprite: a simple, cheat-proof, credit-based system for mobile ad hoc networks', *Proceedings of IEEE INFOCOM 2003*, pp.1987–1997.

Zhu, S., Xu, S., Setia, S. and Jajodia, S. (2003) 'Establishing pair wise keys for secure communication in ad hoc networks: a probabilistic approach', *Proceedings of the 11th IEEE International Conference on Network Protocols (ICNP'03)*, pp.326–335.

Zhuang, S., Lai, K., Stoica, I., Katz, R. and Shenker, S. (2003) 'Host mobility using an internet indirection infrastructure', *Proceedings of First International Conference on Mobile Systems, Applications, and Services (ACM/USENIX Mobisys).*

Zouridaki, C., Mark, B., Hejmo, M. and Thomas R. (2005) 'A quantitative trust establishment framework for reliable data packet delivery in MANETs', *Proceedings of the Third ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, pp.1–10.