International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 01
January 2015

Privacy Protection for decentralized data in military network using CP-ABE

[1]Jada Koteswar Rao & [2]P Eswaraiah
[2]Associate Professor, Department Of computer Science and Engineering .
[1,2] M.Tech BVSR Engineering College ,Chimakurthy – Prakasam .

Abstract-

Wireless sensor networks will be widely used to focused on making these networksfeasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS.SPINS has two secure building blocks: SNEP and TESLA. SNEP includes: data confidentiality, two-party data authentication, andevidence of data freshness. TESLA provides authenticated broadcast for severely resource-constrained environments. We implementedthe above protocols, and show that they are practical even on minimal hard ware: the performance of the protocol suite easily matches thedata rate of our network. Additionally, we demonstrate that the suite can be used for build ing higher level protocols.

Keywords : secure communication protocols; sens or networks; mobile ad hoc networks; MANET; authentication of wireless communication; secrecy and confidentiality; cryptography.

I. Introduction

Battle field management: remote sensors can help eliminatesome of the confusion associated with combat. Theycan allow accurate collection of informat ion about currentbattle field conditions as well as giving appropriate in formationto soldiers, weapons, and vehicles in the battlefield.At UC Berkeley, we think these systems are important, andwe are starting a major initiat ive to explore the use of wirelesssensor networks. security and privacy questions arise if third partiescan read or tamper with sensor data. We envision wirelesssensor networks being widely used .including for emergencyand life-critical systems . and here the questions of securityare foremost.

We envision a future where thousands to millions of smallsensors form self-o rganizing wireless networks. How can weprovide security for these sensor networks? Security is noteasy; compared with conventional desktop computers, severechallenges exist .these sensors will have limited processingpower, storage, bandwidth, and energy.We need to surmount these challenges, because security isso important. Sensor networks will expand to all aspectsof our lives. Here are so me typical applications:

Emergency res ponse information: sensor networks willcollect informat ion about the status of buildings, people,and transportation pathways. Sensor informat ion must becollected and passed on in mean ingful, secure ways toemergency response personnel.

Medical monitoring: we envision a future where individualswith some types of medical conditions receive constantmonitoring through sensors thatmonitor health conditions.For some types of med ical conditions, remote sensors mayapply remedies (such as instant release of emergency med icationto the bloodstream).

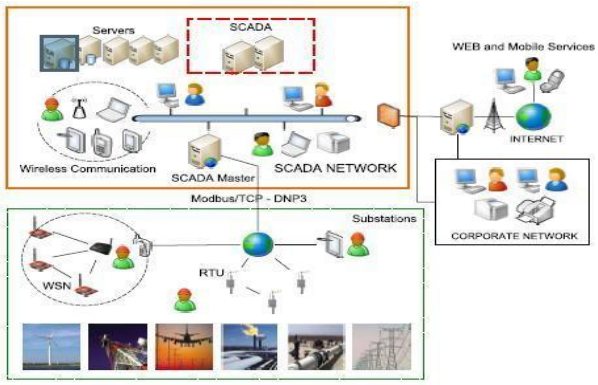

Fig1: Wireless Sensor Network

This article presents a set of Security Protocols for SensorNetworks, SPINS. The chief contributions of this article are:

- Exp loring the challenges for security in sensor networks.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 01
January 2015

- Designing and developing TESLA providing authenticated streaming broadcast.
- Designing and developing SNEP (Secure Network EncryptionProtocol) providing data confidentiality, t wopartydata authentication, and data freshness, with lo woverhead.
- Designing and developing an authenticated routing protocolusing our building blocks.

Data confidentiality

A sensor network should not leak sensor readings to neighboringnetworks. In many applications (e.g., key distribution)nodes communicate highly sensitive data. The standard approachfor keeping sensitive data secret is to encrypt the datawith a secret key that only

intended receivers possess, henceachieving confidentiality. Given the observed communicat ionpatterns, we set up secure channels between nodes and basestations and later bootstrap other secure channels as necessary.

Data authentication

Message authentication is important for many applications insensor networks (including administrative tasks such as networkreprogramming or controlling sensor node duty cycle).Since an adversary can easily in ject messages, the receiverneeds to ensure that data used in any decision-making processoriginates from a trusted source. Informally, data authenticationallows a receiver to verify that the data really was sent bythe claimed sender. Informally, data authentication allo ws areceiver to verify that the data really was sent by the claimedsender.In the two-party communicat ion case, data authenticationcan be achieved through a purely symmetric mechanism: Thesender and the receiver share a secret key to compute a messageauthentication code (MAC) of all communicated data.When a message with a correct MAC arrives, the receiverknows that it must have been sent by the sender.This style of authentication cannot be applied to a broadcastsetting, without placing much stronger trust assumptionson the network nodes. If one sender wants to send authenticdata to mutually un-trusted receivers, using a symmetric MACis insecure: any one of the receivers knows theMAC key, andhence, could impersonate the sender and forge messages toother receivers. Hence, we need an asymmet ric mechanis mto achieve authenticated broadcast. One of our contributionsis to construct authenticated broadcast from symmetric primitivesonly, and introduce asymmetry with delayed key disclosureand one-way function key chains.

II. Related Work

Because of stringent resource constraints on the sensor nodes,imp lementation of the cryptographic primitives is a major challenge. We can sacrifice some security to achieve feasibilityand efficiency, but we still need a core level of strongcryptography. Below we d iscuss how we provide strong cryptographydespite restricted resources.Memory size is a constraint: our sensor nodes have8 Kbytes of read-only program me mo ry, and 512 bytes ofRAM. The program memory is used for TinyOS, our securityinfrastructure, and the actual sensor net application. To saveprogram memory we imp lement all cryptographic primit ivesfrom one single block cipher [2].Block cipher. We evaluated several algorith ms for use as ablock cipher. An init ial choice was the AES algorith m Rijndael[12]; however, after further inspection, we sought alternativeswith smaller code size and higher speed. The baselineversion of Rijndael uses over 800 bytes of lookup tableswhich is too large for our memory-deprived nodes. An optimizedversion of that algorith m (about a 100 t imes faster)uses over 10 Kbytes of lookup tables. Similarly, we rejectedthe DES b lock cipher wh ich requires a 512-entry SBo x tableand a 256-entry table for various permutations [32]. A smallencryption algorith m such as TEA [54] is a possibility, but ishas not yet been subject to cryptanalytic scrutiny.4 We useRC5 [47] because of its small code size and high efficiency.RC5 does not rely onmult iplication and does not require largetables. However, RC5 does use 32-bit data-dependent rotates,which are expensive on our Atmel processor (it only supportsan 8-bit single bit rotate operation).Even though the RC5 algorith m can be expressed succinctly,the common RC5 lib raries are too large to ourplatform. With a judicious selection of functionality, we use asubset of RC5 fro m OpenSSL, and after further tuning of thecode we achieve an additional 40% reduction in code size.Encryption function. To save code space, we use the samefunction for both encryption and decryption. The counter(CTR) mode of block ciphers has this property.CTR mode is a stream cipher. Therefore, the size of the ciphertextis exactly the size of the plaintext and not a mult ipleof the block size. 5 This property is particularly desirablein our environment. Message sending and receiving consumea lot of energy. Also, longer messages have a higherprobability of data corruption. Therefore, block cipher messageexpansion is undesirable. CTR mode requires a counterfor proper operation. Reusing a counter value severely degradessecurity. In addition, CTR-mode offers semantic security. The same plaintext sent at different times is encryptedinto different ciphertext since the encryption pads are generatedfrom different counters. To an adversary who does notknow the key, these messages will appear as two unrelatedrandom strings. Since the sender and the receiver share thecounter, we do not need to include it in the message. If thetwo nodes lose the synchronization of the counter, they cansimply transmit the counter explicit ly to resynchronize usingSNEP with strong freshness.Freshness. Weak freshness

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 01
January 2015

is automatically provided by theCTR encryption. Since the sender increments the counter aftereach message, the receiver verifies weak freshness by verifyingthat received messages have a monotonically increasingcounter. For applications requiring strong freshness, thesender creates a random (an unpredictable 64-b itvalue) and includes it in the request message to the receiver.The receiver generates the response message and includes thenonce in the MAC computation (see section 5). If the MACof the response verifies successfully, the node knows that theresponse was generated after it sent the request message andhence achieves strong freshness.Random-number generation. The node has its own sensors,wireless receiver, and scheduling process, from wh ich wecould derive random digits. But to minimize power requirements,we use a MAC function as our pseudo-random nu mbergenerator (PRG), with the secret pseudo-random numbergenerator key. We also keep a counter that we incrementafter each pseudo-random block.

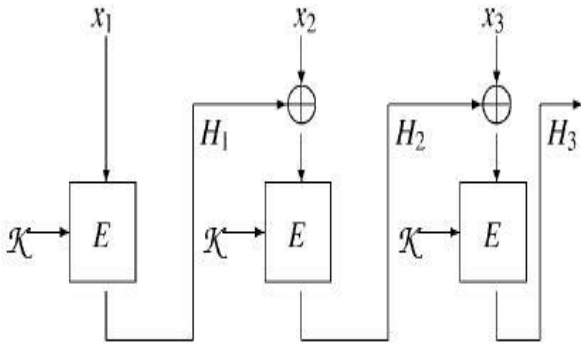

Fig2: MA C Authentication Code

III. Pe rformance Analysis

We evaluate the implementation of our protocols by code size,RAM size, and processor and communicat ion overhead.The code size of three implementationsof crypto routines in TinyOS. The smallest version ofthe crypto routines occupies about 20% of the availab le codespace. The difference between the fastest and the smallest implementationstems fromtwo d ifferent implementations of thevariable rotate function. The TESLA protocol uses another574 bytes. Together, the crypto library and the protocol implementationconsume about 2 Kbytes of program memo ry,wh ich is acceptable in most applications.It is important to identify reusable routines to minimizecall setup costs. For examp le, OpenSSL implements RC5 encryptionas a function. On our sensor hardware, the code sizeof call setup and return outweigh the code size of the body ofthe RC5 function. We implement RC5 as a macro and onlyexpose interfaces to theMAC and CTR-ENCRYPT functions.The performance of the cryptographic primitivesis adequate for the bandwidth supported by the currentgeneration of network sensors. Key setup is relatively expensive(4 ms). In contrast, the fast version of the code uses lessthan 2.5 ms to encrypt a 16 byte message and to compute theMAC (the smaller but slower version takes less than 3.5 ms).Let us compare these time against the speed of our network.Our radio operates at 10 kbps at the physical layer. Ifwe assume that we communicate at this rate, we can performa key setup, an encryption, and a MAC for every message wesend out.In our imp lementation, TESLA discloses the key aftertwo intervals. The stringent buffering requirementsalso dictate that we cannot drop more than one key disclosurebeacon. We require a maximu m of two key setup operationsand two CTR encryptions to check the validity of a disclosedTESLA key. Additionally, we perform up to two key setupoperations, two CTR encryptions, and up to four MAC operationto check the integrity of a TESLA message.7 Thatgives an upper bound of 17.8 ms for checking the bufferedmessages. This amount of work is easily performed on ourprocessor. In fact, the limiting factor on the bandwidth of authenticatedbroadcast traffic is the amount of buffering we candedicate on individual sensor nodes. Table 4 shows the memorysize required by the security modules. We configure theTESLA protocolwith four messages: the disclosure intervaldictates a buffer space of three messages just for key disclosure,and we need an additional buffer to use this primitive ina more flexible way. Despite allocating min imal amounts ofmemory to _TESLA, the protocols we implement consumehalf of the available memo ry, and we cannot afford any morememory.Energy costs. We examine the energy costs of securitymechanisms. Most energy costs will come fro m ext ra transmissionsrequired by the protocols.Remaining security issues. Although this protocol suite addressesmany security related problems, there remain manyadditional issues. First, we do not address the problem of informationleakage through covert channels. Second, we donot deal completely with compro mised sensors, we merelyensure that compro mising a single sensor does not reveal thekeys of all the sensors in the network. Third, we do not dealwith denial-o f-service (DoS) attacks in this work. Since weoperate on a wireless network, an adversary can always performa DoS attack by jamming the wireless channel with astrong signal. Finally, due to our hardware limitations, wecannot provide Dife-Hellman style key agreement or usedigital signatures to achieve non - repudiation. For the majo rityof sensor network applications, authentication is sufficient.

Authenticated Routing

Using the TESLA protocol, we developed a lightweight, authenticatedad hoc routing protocol that builds an authenticatedrouting topology. Ad hocPage 3 routing has

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 01
January 2015

been an active area of research [11]. Marti et al. d iscussa mechanism to protect an ad hoc network against misbehavingnodes that fail to forward packets correctly [28]. Theydescribe two mechanis ms: a watchdog to detect misbehavingneighboring nodes, and a pathrater to keep state about thegoodness of other nodes. They propose running these mechanismson each node. However, we are not aware of a routingprotocol that uses authenticated routing messages. It is possiblefor a malicious user to take over the network by injectingerroneous, replaying old, or advertise incorrect routing information.The authenticated routing scheme we developed mitigatesthese problems.The routing scheme within our prototype network assumesbidirectional co mmun ication channels. The route discovery dependson periodic broadcast of beacons. Every node, uponreception of a beacon packet, checks whether it has alreadyreceived a beacon (which is a normal packet with a globallyunique sender ID and current t ime at base station, protectedby a MAC to ensure integrity and that the data is authentic)in the current epoch.8 If a node hears the beacon within theepoch, it does not take any further action. Otherwise, the nodeaccepts the sender of the beacon as its parent to route towardsthe base station. Additionally, the node would repeat the beaconwith the sender ID changed to itself. This route discoveryresembles a distributed, breadth first search algorithm, andproduces a routing topology.However, in the above algorithm, route discovery dependsonly on the receipt of route packet, not on its contents.It is easy for any node to claim to be a valid base station.In contrast, we note that the TESLA key disclosure packetscan easily function as routing beacons. We accept only thesources of authenticated beacons as valid parents. Receptionof a TESLA packet guarantees that that packet originated atthe base station, and that it is fresh. For each time interval, weaccept as the parent the first node sending a successfully authenticatedpacket. Combin ing TESLA key disclosure withdistribution of routing beacons allows us to combine transmissionof the keys with network maintenance.We have outlined a scheme leading to a lightweight authenticatedrouting protocol for sensor networks. Since eachnode accepts only the first authenticated packet as the one touse in routing, it is impossible for an attacker to reroute arbitrary lin ks within the sensor network. Each node verifies thebehavior of the parent by imp lementing functionality similarto watchdogs described in [8].The authenticated routing scheme above is just one way tobuild authenticated ad hoc routing protocol using TESLA.In protocols where base stations are not involved in route construction,TESLA can still be used for security. In these cases, the initiating node will temporarily act as base station and beacons authenticated route updates.

Node-to-node key agreement

A convenient technology for bootstrapping secure connectionsis to use public key cryptography protocols for symmetrickey setup [2]. Unfortunately, our resource constrainedsensor nodes prevent us from using computationally expensivepublic key cryptography. We need to construct our protocolssolely fro m symmet ric key algorith ms. We design a symmetricprotocol that uses the base station as a trusted agent forkey setup.Assume that the node wantsto establish a shared secretsession key .

$$
\begin{aligned}
A \to B:&\quad N_A, A,\\
B \to S:&\quad N_A, N_B, A, B, \mathsf{MAC}\left(K'_{BS}, N_A|N_B|A|B\right),\\
S \to A:&\quad \{\mathcal{SK}_{AB}\}_{K_{SA}}, \mathsf{MAC}\left(K'_{SA}, N_A|B|\{\mathcal{SK}_{AB}\}_{K_{SA}}\right),\\
S \to B:&\quad \{\mathcal{SK}_{AB}\}_{K_{SB}}, \mathsf{MAC}\left(K'_{SB}, N_A|B|\{\mathcal{SK}_{AB}\}_{K_{SB}}\right).
\end{aligned}
$$

The protocol uses our SNEP protocol with strong freshnessthat the key was really generated by the base station. Notethat the MAC in the second protocol message helps defendthe base station from denial-of-service attacks, and the basestation only sends two messages to and if it received alegitimate request from one of the nodes.A nice feature of the above protocol is that the base stationperforms most of the transmission work. Many other protocolsinvolve a ticket that the server sends to one of the partieswhich forwards it to the other node, which requires mo re energyfor the nodes to forward the message.The Kerberos key agreement protocol achieves similarproperties, but it does not provide strong key freshness[17,13]. If Kerberos used SNEP with strong freshness, thenKerberos would have greater security. The key distribution for resourcestarveddevices in a mobile environ ment [5]. Park et al. [7]point out weaknesses and improvements. Beller and Yacobifurther develop key agreement and authentication protocols[4]. Boyd and Mathuria survey the previous work on key distributionand authentication for resource-starved devices inmobile environments [8]. The majo rity of these approachesrely on asymmet ric cryptography. Bergstrom et al. considerthe problem of secure remote control of resource-starved devicesin a home [6].Fo x and Gribble present a security protocol providing secureaccess to application level pro xy services [16]. Theirprotocol is designed to interact with a proxy to Kerberos andto facilitate porting services relying on Kerberos to wire lessdevices.The work of Patel and Cro wcroft focuses on security solutionsfor mobile user devices [39]. Unfortunately, their workuses asymmetric cryptography and is,Page 4 hence, too expensivefor the environments we envision.The work of Czerwinski et al. also relies on asymmetriccryptography for authentication [10].Stajano and Anderson discuss the issues of bootstrappingsecurity devices [51]. Their solution requires physical contactof the new device with a master device to imp rint the trustedand secret informat ion.Zhou and Haas propose to secure ad hoc networks usingasymmet ric cryptography [57]. Recently,

Basagni et al.proposed to use a network-wide sy mmetric key to secure anad hoc routing protocol [2]. While this approach is efficient,it does not resist compro mise of a single node.Carman et al. analyze a wide variety of approaches forkey agreement and key distribution in sensor networks [9].They analyze the overhead of these protocols on a variety ofhardware platforms.Marti et al. discuss a mechanis m to protect an ad hoc networkagainst misbehaving nodes that fail to forward packetscorrectly [28]. They propose that each node runs a watchdog(to detect misbehaving neighboring nodes) and a pathrater (tokeep state about the goodness of other nodes); their solution,however, is better suited for traditional networks, with emphasison reliable po int-to-point communication, than to sensornetworks.Hubau x et al. present a system for ad hoc peer-to-peer authenticationbased on public key cert ificates [24]. They consideran ad hoc network with nodes powerful enough for performingasymmetric cryptographic operations.

IV. Conclusion

We designed and built a security subsystem for an extremelylimited sensor network platform. We have identified and imp lementeduseful security protocols for sensor networks: authenticatedand confidential communicat ion, and authenticatedbroadcast. We have imp lemented applications includingan authenticated routing scheme and a secure node-to-nodekey agreement protocol.Most of our design is universal and applicable to other networksof low-end devices. Our primitives only depend on fastsymmetric cryptography, and apply to a wide variety of deviceconfigurations. On our limited platform energy spentfor security is negligible compared with to energy spent onsending or receiving messages. It is possible to encrypt andauthenticate all sensor readings.The communicat ion costs are also small. Data authentication,freshness, and confidentiality properties use up a net6 bytes out of 30 byte packets. So, it is feasible to guaranteethese properties on a per packet basis. It is difficult to imp roveon this scheme, as transmitting a MAC is fundamentalto guaranteeing data authentication.Certain elements of the design were theavailab le experimental platform. If we had a more powerfulplatfo rm, we could have used block ciphers other thanRC5. The emphasis on code reuse is another property forcedby our platform. A more powerful device would allow mo remodes of authentication. In particular, memory restrictionson buffering limit the effective bandwidth of authenticatedbroadcast.Despite the shortcomings of our target platform, we built asystem that is secure and works. With our techniques, we believesecurity systems can become an integral part of practicalsensor networks.

REFERENCES

[1] J. Peerenboom and R. Fisher, “Analyzing Cross - Sector Interdependencies”,IEEE Co mputer Society,

HICSS, IEEE Co mputer Society, pp. 112–119, 2007. [2] Zig Bee Alliance, http://www.zigbee.org/,accessed on February, 2010.

[3]WirelessHART, ttp://WirelessHART.hartcomm.org/,HA RT

Co mmunicat ionFoundation, accessed on February, 2010.

[4] ISA100, “Wireless Systems for Automat ion”, http://www.isa.org/ Content/NavigationMenu/Technical*n*Informat ion/AS CI/ISA100*n* Wireless*n*Comp liance*n*Institute/ISA100*n*

Wireless*n*Comp liance*n*Institute.htm,accessed on February, 2010.

[5] Modbus -IDA,“The Architecture for Distributed Automation”, http://www.modbus.org/, accessed on February, 2010.

[6] DNP3,“DNP Users Group”, http://www .dnp.org, accessed on February,2010.

[7] HART Co mmunication, http://www.hartco mm2.org, accessed on February,2010.

[8] J. Lopez, R. Ro man and C. Alcaraz,“Analysis of Security Threats,Requirements, Technologies and Standards in Wireless Sensor Network”,Found ations of Security Analysis and Design V , LNCS 5705, pp. 289–338, Springer, 2009.

[9] R. Ro man, C. A lcaraz and N. Sklavos, “On the Hardware Implementation Efficiency of Criptographic Primitives”, Wireless Sensor NetworkSecurity, Cryptology and Informat ion Security Series, vol. 1, pp. 285–305, 2008.

[10] IEEE 802.15.4-2006,“IEEE Standard for Information technology-Telecommunicat ions and informat ion exchange between systems -Localand metropolitan area networks”,http://standards.ieee.org/getieee802/downl oad/802.15.4-2006.pdf, 2006.

[11] D. Johnson, D.A. Maltz and J. Broch, The dynamic source routing protocolfor mobile ad hoc Page 5 networks, Internet draft, Mobile Ad-Hoc Network(MANET) Working Group, IETF (1999).

[12] J. Daemen and V. Rijmen, A ES p roposal: Rijndael (1999).

[13] Dallas, iButton: A Java-powered cryptographic iButton, http://www.ibutton.com/ibuttons/java.html [14] W. Dif_e and M.E. Hellman, Privacy and authentication: An

introductionto cryptography, Proceedings of the IEEE 67(3) (1979) 397.427.

[15] Fortezza, Fortezza: Application imp lementers guide (1995).

[16] A. Fo x and S.D. Gribble, Security on the move: Indirect authenticationusing Kerberos, in: International Conference on Mobile Co mputingand

Networking (MobiCo mÕ96) (1996) pp. 155.164. [17] R. Gennaro and P. Rohatgi, How to sign digital streams, in: Advancesin Cryptology Đ CryptoÕ97, Lecture Notes in Computer Science, Vo l.1294 (1997) pp. 180.197.

[18] O. Goldreich, S. Go ldwasser and S. Micali, How to construct randomfunctions, Journal of the ACM 33(4) (1986) 792.807.

[19] S. Go ldwasser and S. M icali, Probabilistic encryption, Journal of Co mputerSecurity 28 (1984) 270.299.

[20] Z. Haas and M. Perlman, The Zone Routing Protocol (ZRP) for ad hocnetworks, Internet draft, Mobile Ad-Hoc Network (MANET) Working Group, IETF (1998).

[21] N.M. Haller, The S/KEY one-time password system, in : Sy mposium onNetwork and Distributed Systems Security (1994).

[22] D. Harkins and D. Carrel, The Internet key exchange (IKE), RFC2409, Informat ion Sciences Institute, University of Southern California(1998).

[23] J. Hill, R. Szewczyk, A.Woo, S. Hollar, D. Culler and K. Pister, Systemarchitecture direct ions for networked sensors, in: International Conferenceon Architectural Support for Programming Languages and OperatingSystems.

[24] J.-P. Hubaux, L. Buttyán and S. C_ apkun, The quest for security in mobilead hoc networks, in: ACMSy mposium on Mobile Ad Hoc Networkingand Co mputing (2001).

[25] D.B. Johnson and D.A. Maltz, Dynamic source

routing in ad hoc wirelessnetworks, in: Mobile Co mputing (Kluwer Academic, 1996) chapter5, pp. 153.181.

[26] Y.-B. Ko and N. Vaidya, Location -Aided Routing (LA R) in mobile adhoc networks, in: International Conference on Mobile Co mputing andNetworking (MobiCo mÕ98) (1998).

[27] J. Kohl and C. Neu man, The Kerberos network authentication service(V5), RFC 1510 (1993).

[28] S. Marti, T. Giu li, K. Lai and M. Baker, Mitigating routing misbehavior inmobile ad hoc networks, in: International Conference on MobileCo mputing and Networking (MobiCo m 2000) (2000) pp. 255.265.

[29] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, Handbook of AppliedCryptography (CRC Press, 1997).

[30] S.P.Miller, C. Neu man, J.I. Sch iller and J.H. Salt zer, Kerberos authenticationand authorizat ion system, Project Athena Technical Plan (1987).