SECURE AD-HOC ROUTING THROUGH A-CODES

Giovanni Schmid[1] and Francesco Rossi[2]
[1]*High Performance Computing and Networking Institute (ICAR), Naples, Italy*
[2]*University of Naples Parthenope, Naples, Italy*

Keywords: Message authentication, Secure routing, Ad-hoc wireless networks.

Abstract: Wireless ad-hoc networks are very attractive in several application domains, but the very nature of these networks and their cost objectives pose big security challenges, perhaps making them the most difficult networking environments to secure. A particular challenging issue is that of secure routing. In this work we propose to get secure routing for such networks through a special coding technique at the physical layer of radio communication channels. This approach has the main advantage of being applicable to any routing protocol, without requiring modifications to the protocol itself, but with a suitable key management. We illustrate it for the concrete case of AODV, the standard routing protocol for Low-data-Rate Wireless Personal Area Networks (LR-WPANs). The resulting analysis seems to indicate that such approach is very promising for LR-WPANs, both in term of performance and energy efficiency.

1 INTRODUCTION

Wireless ad-hoc networks are very attractive for many applications, but the absence of a fixed infrastructure, the adaptivity and time-varying shape of their interconnection meshes, together with the physical characteristics of the radio channel, combine to create significant challenges, perhaps making them the most difficult networking environments to secure. In addition, node devices have limited capabilities in terms of computing power, available storage, and power drain, putting severe limits on the security overhead these networks can tolerate, something that is of far less concern with higher bandwidth networks.

A particular challenging issue for wireless ad-hoc networks is that of designing both secure and efficient routing protocols. The reason for that is twofold. First, there are a variety of ad-hoc wireless networks (e.g. sensor networks, vehicular networks) and usage scenarios (e.g. ambient monitoring, industry control), so it is impossible to provide a single routing protocol fitting each need. Last but not least, the design of reliable and efficient secure routing protocols for real-word applications has resulted to be an elusive issue.

These difficulties are undoubtedly reflected by current emerging industry standards. The ZigBee Alliance[1] simply adopts the Ad hoc On Demand Distance Vector (AODV) routing protocol (Perkins et al., 2003), which does not provide any authentication mechanism at all, and is vulnerable to many attacks (Sanzgiri et al., 2002; Ning and Sun, 2003).

In this work, we propose to secure routing in wireless ad-hoc networks through A-coding. The A-code primitive was introduced in (Schmid and Rossi, 2010) to allow for the establishment of authentic public keys in wireless sensor networks. Here, we exploit A-coding directly at the physical layer of the radio communication channel, as a low level message authentication processing. This approach turns out in offering hop-by-hop message authentication to any routing protocol without requiring modification to the protocol itself, but just providing appropriate key management at the network layer.

We illustrate the A-coding approach for the concrete case of AODV, sketching a comparison with the coding techniques of the IEEE Standard 802.15.4 (IEEE, 2006), which has been adopted by ZigBee for the specifications of the medium access control sublayer (MAC) and the physical layer (PHY) of the LR-WPAN protocol stack. The resulting analysis seems to indicate that such approach is very promising for LR-WPANs, both in term of performance and energy efficiency.

The rest of the paper is organized as follows. Sec-

[1] An association of companies founded in 2003 and committed in defining the protocol stack for low-data-rate, wireless networks (LR-WPANs); http://www.zigbee.org

Schmid G. and Rossi F..
SECURE AD-HOC ROUTING THROUGH A-CODES.
DOI: 10.5220/0003137015101156
In *Proceedings of the 1st International Conference on Pervasive and Embedded Computing and Communication Systems* (PECCS-2011), pages 151-156
ISBN: 978-989-8425-48-5

tion 2 discusses about related work, whilst Section 3 describes the A-code primitive. In Section 4 we show how to secure AODV thanks to A-coding. Section 5 sketch a comparison with the 802.15.4, and discusses general A-code key management issues for AODV. Finally, in Section 6 we draw out our conclusions, and illustrate our future work.

2 RELATED WORK

Attacks against routing can be realized through a suitable combination of offensive techniques such as eavesdropping, identity spoofing, and the replay, modification, forgery or deletion of routing control packets. The adaptive nature of the communication mesh in ad-hoc networks, along with node's constrained resources, compel the adoption of on-demand routing, which in case of wireless communications is particularly exposed to such offensive techniques.

Many secure routing protocols for wireless ad-hoc networks, based on both private-key and public-key cryptography, have been proposed by the research community over the last decade, with alternate results as in (Sanzgiri et al., 2002; Zapata and Asokan, 2002; Papadimitratos and Hass, 2003). Reporting on such proposals is outside the scope of this work. A comprehensive survey of secure on-demand routing is given in (Hu and Perrig, 2004), whilst (Karlof and Wagner, 2003) describes attacks on sensor network routing protocols, and introduces some generic countermeasures.

In virtually all cases, strategies have been adopted to face against node's constrained resources and achieve acceptable overheads. Those approaches, not surprisingly, have often resulted in some security weakness or in assumptions that are difficult to be satisfied in practice (Ramachandran and Yasinsac, 2001). For example, in (Sanzgiri et al., 2002; Hu et al., 2003; Hu et al., 2005) authentication is realized only for routing control packets, exposing data packets to serious threats. Both SAODV (Zapata and Asokan, 2002) and ARAN (Sanzgiri et al., 2002) provide message authenticity only when all intermediate nodes are trustworthy, which is an overly restrictive assumption. The TESLA authentication framework (Perrig et al., 2000) - along with its variant μTESLA (Perrig et al., 2002), specifically designed for wireless sensor networks, avoid hop-by-hop authentication by relying on loosely time synchronized network nodes. However, secure time synchronization has been demonstrated to be very difficult to achieve, also on networks with a fixed infrastructure (Menezes, et al.,1996). Consequently, all the routing protocols based on such frameworks (e.g. the protocol in SPINS (Perrig et al., 2002), SEAD (Hu et al., 2003), SEAR (Zhao et al., 2008)) suffer the same drawback.

Considered together, the above works and experiences seem to indicate that effective secure protocols for ad-hoc routing can only be achieved if hop-by-hop authentication is guaranteed for all the packets involved in the protocol. Both LHAP (Zhu et al., 2003) and HEAP (Akbani et al., 2008) were designed to offer hop-by-hop authentication for data packet as well as control packets. LHAP realizes message authentication through one-way hash key chains, and that turns out in a low efficiency in terms of memory requirements, since long time communications requires long chains. HEAP is a modified version of the HMAC algorithm that uses two keys and seems very efficient for multicast communications. HEAP was designed to defend against attacks originating from nodes that are not authenticated members of the network (*outsider attacks*).

The A-coding approach offers hop-by-hop authentication, too, and in the same security assumptions than HEAP. However, it has one main advantage: since hop-by-hop authentication is realized at the lowest layer of the protocol stack, any protocol can get its own proper authentication service by just being coupled with suitable key management, without any modification to the protocol itself.

A-codes are based upon I-codes (Cagalj et al., 2006) and, like these ones, were introduced to allow for the establishment of authentic public keys over insecure radio channels (Schmid and Rossi, 2010). Differently than I-codes, however, A-codes can provide authentication without user intervention and in the absence of special, dedicated radio-frequency channels (*integrity channels*).

3 THE A-CODE PRIMITIVE

The A-code primitive was introduced in (Schmid and Rossi, 2010) to allow for the establishment of authentic public keys in wireless sensor networks. It can operate directly at the physical layer of the protocol stack, on PPDUs[2], offering a "physical coding" alternative to traditional message authentication codes (MACs).

In A-codes, message integrity is gained through unidirectional message coding and on-off keying communication with signal anti-blocking; these are

[2]PPDU stands for PHY Protocol Data Unit, and represent the message structure managed by the IEEE Standard 802.15.4 (IEEE, 2006) physical (PHY) layer.

the three components which give rise to Integrity Codes (Cagalj et al., 2006).

Unidirectional message coding ensures that bit 0 cannot be changed in bit 1. Manchester code is an example of unidirectional coding scheme; it encodes each bit 1 as 10 and each bit 0 as 01. If we suppose that an adversary can only convert a bit 0 into bit 1, then the receiver will be able to detect forged messages, since such messages cannot be decoded properly.

On-off keying (OOK) is a signal modulation technique such that bit 1 is transmitted as the presence of a signal, and bit 0 as the absence of a signal for a known time slice. *Signal anti-blocking* uses a random energy signal, so that an adversary cannot annihilate bits 1 by jamming the signal. Considered together, on-off keying and signal anti-blocking give a good resistance against attacks based upon jamming and/or bit-flipping.

I-Codes can also achieve message authentication, but only through presence awareness. That is, the receiver needs to be aware of the fact that the received signal is on the channel used by an authorized sender. This requires an infrastructure of authorized senders located in known positions or, alternatively, continuously signaling senders on known channels. Of course, these two conditions are not usually satisfied in case of LR-WPANs.

In A-codes, authentication for each single PPDU is provided by expanding some of its bits into pseudo-random strings $p(n)$ given by:

$$\begin{aligned} p(n) &= H(K\|H(K\|H(....H(K\|X_{ID})....))) \\ &= H(K\|p(n-1))\,. \end{aligned} \quad (1)$$

In (1), X_{ID} denotes the identifier of node X, H is a suitable and known cryptographic hash function, n is an integer related is some way to the number of expanded bits sent so far by node X to the receiver node Y, and K is a secret key shared between X and Y. The function H is applied iteratively n times. The receiver Y will consider a given PPDU authentic only if:

$$H(K\|p'(n-1)) = p(n)\,, \quad (2)$$

for any of the values of n corresponding to one of the expanded bits in such PPDU. In equation (2) p' represents the pseudo-random string as computed by Y, whereas - because of the message integrity property assured by OOK with unidirectional coding and signal antiblocking - $p(n)$ is the pseudo-random string issued by X. The first member of (2) can be computed by Y as a consequence of its knowledge of H, K, X_{ID} and n. Since the value of n has not to be kept secret, the synchronization between X and Y can be easily obtained by sending that value in clear from X to Y in each PPDU. For efficiency and easy of implementation, only a constant, small number of bits at prescribed off-set positions in each PPDU should be expanded through (1). Actually, because of the integrity property of PPDUs, just one single bit could be expanded for each PPDU; however, noisy channels could require a slightly greater number of hash expansions to avoid denial of service conditions.

4 SECURING AODV

In this section we illustrate how to secure the AODV routing protocol with the A-Code primitive. Our arguments could have been easily exposed for the general case of (on-demand) routing protocols, without any substantial modification. However, AODV is one of the most prominent protocols for ad-hoc wireless networks, and discussing it explicitly will allow us to be more specific in the description of our technique and to sketch a comparison, in terms of bit rate throughput, with the modulation techniques provided for the ZigBee protocol stack.

AODV is based on three standard routing messages (see Figure 1): route request (RREQ), route replay (RREP) and route error (RERR). The RREQ packet is used when a route to a new destination is needed: the source node broadcasts an RREQ packet to find a route to the destination. The route is made available by unicasting a RREP packet back to the originator of the RREQ. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node that is able to satisfy the request. A RERR message is used when a link break in an active route is detected, in order to notify other nodes that some destinations are no longer reachable by way of the broken link. The format lengths for RREQ, RREP and RERR messages in AODV are of 24, 20 and 20 bytes, respectively.

We limit our description of A-coding to RREQ packets, since the other two cases are very similar. The A-coding workflow composes of the following steps (see Figure 2):

1. The first step consists in encapsulating in a source PPDU the MAC data frame (MPDU) containing the RREQ packet as its own MAC payload field. We remark that during this phase nor the RREQ packet is modified, neither specific fields are required in the MPDU. The output is a PPDU which has the same structure and similar information encoding as prescribed by IEEE Standard 802.15.4, but has a slightly modified synchro-

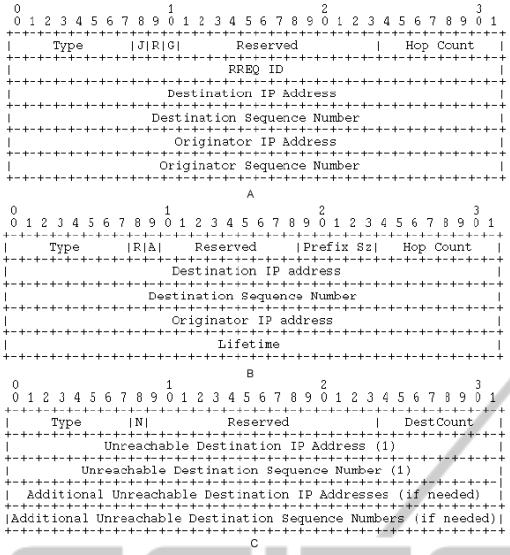

Figure 1: Route Request (RREQ), Route Replay (RREP) and Route Error (RRER) message formats for AODV.

nization header SHR', which replaces the IEEE SHR for transceiver synchronization in A-coding mode;

2. According to the information encoded in SHR', m bits (the figure shows the case $m = 3$) at prescribed offset positions in the source PPDU are expanded into hash digests of size $|H|$ given by (1). The output of this phase is an "expanded" PPDU which is $m|H|$ bytes longer than the source PPDU;
3. After the expansion through hash digests, the PPDU is coded thanks to an unidirectional coding scheme. For Manchester scheme the *rate* is $r = 2$, but schemes exist such that $r \leq 1.5$;
4. Finally, the bits constituting the output chip stream from the previous phase are modulated by using OOK with signal antiblocking. The length of the chip stream is given by $r(|SHR'| + |PHR| + |PSDU| + m|H|)$, where the three first addendums are the lengths of the (modified) synchronization header, the PHY header and the PHY payload, respectively.

5 PERFORMANCE AND SECURITY ISSUES

In order to show the viability of our approach, this section discusses about performance and security goals of A-codes. Section 5.1 gives a performance comparison of A-coding versus the related techniques encompassed by IEEE Standard 802.15.4, which - as

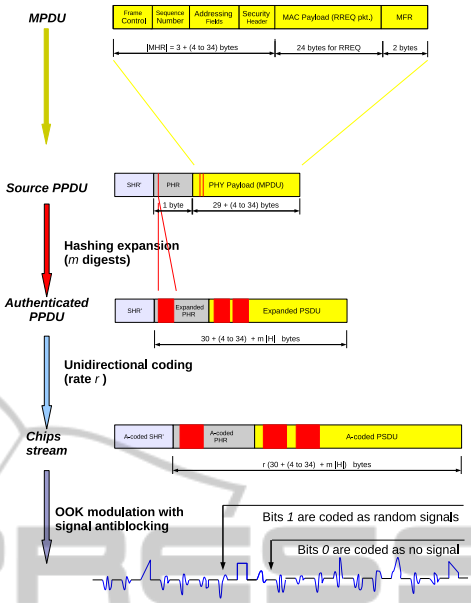

Figure 2: A-Coding workflow for the RREQ packet of AODV.

we told in the introduction - defines the medium access sublayer (MAC) and physical layer (PHY) specifications for the LR-WPAN protocol stack. Different alternatives exist in setting up cryptographic keys in view of node authentication, which affect the dependability of the network. This issue is briefly discussed in Section 5.2 for the case of securing AODV through A-codes.

5.1 A-coding versus IEEE 802.15.4

IEEE PHY layer (IEEE, 2006) uses spread-spectrum modes of communication to obtain some resilience to jamming and improved noise immunity. In alternative to spread spectrum, A-codes use the spreading technique illustrated in Section 4, so in both cases it is possible to consider the *spread factor* (*SF*), that is the ratio of the chipstream length to that of its related source PPDU. The spread factor is a measure of loss in data throughputs w.r.t. the rates at which a transceiver can receive and transmit chips. Thus, the *gain factor*

$$\gamma = \frac{SF_I}{SF_A}$$

can be used to compare the performance, in term of data rates, of a given IEEE coding technique (I) versus the A-coding one (A), assuming that a transceiver can perform at roughly the same chipstream rates for I and A. A value $\gamma < 1$ indicates that the considered IEEE technique outperforms A-coding, and viceversa. Figure 3 reports the value of γ relative to the

RREQ packet of AODV for all the coding techniques at the PHY layer (IEEE, 2006). Those values were computed for a unidirectional code of rate $r = 1.5$ and for a number of $m = 1,2,3$ bits subjected to an hash digest expansion of 128 bits. For the figures, we assumed for simplicity $|SHR| = |SHR'|$, and $|MHR| = 7$ (see Section 4).

PHY type	Frequency Band (MHz)	IEEE Spreading factor	*Gain Factor* for the RREQ packet in AODV		
			m = 1	m = 2	m = 3
868/915 PBSK	868–868.6 / 902–928	15	3.66	2.24	1.62
2450 O-QPSK	2400-2483.5	8	1.95	1.20	0.86
915 ASK	902–928	6.4	1.49	0.91	0.65
868/915 O-QPSK	868–868.6 / 902–928	4	0.98	0.60	0.43
868 ASK	868–868.6	1.6	0.45	0.29	0.21

Figure 3: Values of the gain factor γ of A-coding w.r.t. the coding techniques encompassed by the IEEE Standard 800.15.4 PHY layer.

Figure 3 shows that in many cases A-coding outperforms spread-spectrum modes of coding. When that does not occur (as in the case of 868 ASK, because of its very low spreading factor of 1.6), the A-coding performance, however, widely falls in the admissible data-ranges for LR-WPANS. Indeed, the data rate achieved in the worst case ($m = 3$) for an OOK modulation performed at only 300 Kchip/s is of 32.4 Kb/s, an improvement of more than 60% on the lower bound (20 Kb/s) prescribed by the standard.

On the other hand, OOK transceivers are nowadays on the market that support data rates of hundreds of Kb/s. These transceivers are cheap and have very low power consumptions, because of the simplicity of OOK implementation and the fact that devices can save on transmit power when sending '0's as no signal. As a matter of fact, OOK modulation is emerging as the optimal choice in short-range, battery-operated wireless applications such as wireless sensor networks.

5.2 Key Management

Authentication through A-codes relies ultimately upon the secret key K (see equation 1), and the way K is established, shared and managed by the network nodes relates to the threat model assumed for that network, resulting in different levels of security. As a general matter of fact, it is unpractical to achieve security in an absolute sense (if any); rather, the point is to get a good trade-off between protection, usability and performance. Discussing the many proposals and contributions given in the literature on the issue of (secret) key set up and management is by far out the scope of this work. We sketch here just few considerations for the specific case of AODV, under the underlying assumption that only outsider attacks are possible[3].

A very simple possibility is to use the same key K for all nodes in the network. In this case K plays the role of a *network key*, and key management can be very lightweight by loading a first key instance on each node during the deployment stage, and then updating it at scheduled times via broadcast communication. With this scheme, thanks to A-codes each node in the network has corroborate evidence that a receiving packet is fresh and was generated by another node in the network[4]. Moreover, this scheme implicitly supports multicast communications, which is the case for any RREQ request and any RERR message.

Against the above advantages, this scheme suffers however the following three main drawbacks: (a) breaking the key may turn out in the compromission of the entire network; (b) detecting and locating unauthorized routing paths and functions can be very difficult, and; (c) it is very expensive to recover from a compromission.

Thus, sensitive usage contexts and exposed environments require a more complex (and resource consuming) key management schema, with one or more keys for each node. A standard approach is that of using different kinds of key, each one with its specific protection role and its own establishment and management protocols (Menezes et al., 1996). In all these cases, the key K in expression (1) should play the role of a *link key* in case of unicast communications (as for RREP packets), and of a *group key* in case of multicast communications (i.e., RREQ and RERR packets). In the first case, an instance for K will be generated and shared only among two one-hop-neighbouring nodes, with the scope of authenticating the communication link between them. In the second case, instead, K will be shared among a given node X and all its one-hop neighbours, in order to authenticate the packets from X.

[3]By the way, the best one can do in facing *insider attacks*, that is attacks by nodes running malicious code or adversaries who have stoled the key material, is to provide for intrusion detection and failure detection.

[4]The parameter n in expression (1) plays a crucial role here, since it assures that unauthorized nodes cannot perform packet relying and replaying.

6 CONCLUSIONS AND FUTURE WORK

In this work we propose to secure routing in wireless ad-hoc networks through A-coding, a special coding technique which operates directly at the physical layer of the radio communication channel. A-coding acts as a low level message authentication processing, and constitutes an alternative to traditional message authentication codes. A performance comparison of A-coding versus the related coding techniques encompassed by IEEE 802.15.4, the adopted standard for low-data-rate, wireless networks, shows the effectiveness of this approach. On the other hand, A-coding relies on OOK modulation, and OOK transceivers are nowadays on the market that have very low costs and power consumptions.

Our future work will be focused on a prototypal implementation of A-coding as firmware in a commercial off-the-shelf transceiver, in order to carry out a testbed for the adoption of this technology.

REFERENCES

Akbani, R., Korkmaz, T., and Raju, G. (2008). HEAP: A packet authentication scheme for mobile ad-hoc networks. *Ad Hoc Networks*, 6(7).

Cagalj, M., Hubaux, J., Capkun, S., Rengaswamy, R., Tsigkogiannis, I., and Srivastava, M. (2006). Integrity (i) codes: Message integrity protection and authentication over insecure channels. In *Proceedings of the 2006 IEEE Symphosium on Security and Privacy*. IEEE.

Hu, Y., Johnson, D., and Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 1(1).

Hu, Y. and Perrig, A. (2004). A survey of secure wireless ad hoc routing. *Security & Privacy*, 2(3).

Hu, Y., Perrig, A., and Johnson, D. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, 11(1-2).

IEEE (2006). *Std IEEE 802.15.4 - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*.

Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(1-2).

Menezes, A., van Oorschot, P., and Vanstone, S. (1996). *Hanbook of Applied Cryptography*. CRC Press.

Ning, P. and Sun, K. (2003). How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols. In *Information Assurance Workshop 2003*. IEEE.

Papadimitratos, P. and Hass, Z. (2003). Secure routing for mobile ad hoc networks. *Mobile Computing and Communications Review*, 7(1).

Perkins, C., Belding-Royer, E., and Das, S. (2003). *RFC 3561 - Ad Hoc On Demand Distance Vector (AODV) Routing*. IETF.

Perrig, A., Canetti, R., Tygar, D., and Song, D. (2000). Efficient authentication and signing of multicast streams over lossy channels. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*. IEEE.

Perrig, A., Szewcyzk, R., Tygar, J., Wen, V., and Culler, D. (2002). SPINS: security protocols for sensor networks. *Wireless Networks*, 8(5).

Ramachandran, P. and Yasinsac, A. (2001). Limitations of on demand secure routing protocols. In *Workshop on Information Assurance*. IEEE.

Sanzgiri, K., Dahill, B., Levine, B., Shields, C., and Belding-Royer, E. (2002). A secure routing protocol for ad hoc networks. In *Proceedings of the 10th IEEE International Conference on Network Protocols*. IEEE.

Schmid, G. and Rossi, F. (2010). A-code: A new crypto primitive for securing wireless sensor networks. In *Proceedings of the First International Workshop on Trust management in P2P Systems*. Springer.

Zapata, G. and Asokan, N. (2002). Securing ad hoc routing protocols. In *Proceedings of the 1st ACM workshop on Wireless security*. ACM.

Zhao, M., Walker, J., Hu, Y., Perrig, A., and Trappe, W. (2008). SEAR: A secure efficient ad hoc on demand routing protocol for wireless networks. In *Proceedings of ASIACSS '08*. ACM.

Zhu, S., Xu, S., Setia, S., and Jajodia, S. (2003). LHAP: a light-weight hop-by-hop authentication protocol for ad-hoc networks. In *Proceedings of the 23rd ICDCS Workshop*. IEEE.