On Secure Communication over Wireless Sensor Networks

Stefan Rass[1] and Michał Koza[2]
[1] *Institute of Applied Informatics, Universität Klagenfurt, Universitätsstrasse 65-67, 9020 Klagenfurt, Austria*
[2] *Faculty of Fundamental Problems of Technology, Wrocław University of Technology, Wrocław, Poland*

Keywords: Wireless Sensor Network, Security: Secrecy, Secret Sharing, Perfectly Secure Message Transmission.

Abstract: This paper investigates (perfectly) secure message transmission over a wireless sensor network. Using a layered network architecture and a very simple form of routing, we show how to construct an arbitrarily secure communication channel over a given infrastructure of wireless devices. Our construction is computationally cheap and requires no cryptographic primitive beyond symmetric encryption on the channels. The security of the transmission can be made arbitrarily strong (in an information-theoretic sense).

1 INTRODUCTION

Secret message transmission is doubtlessly an important aspect in vast amount of communication scenarios, and has been thoroughly studied in the wired domain for decades. The increasing interest and expanding range of applications in the wireless domain sheds a different light on security requirements when designing wireless transmission protocols. In this work, we propose a simple protocol for transmission over a wireless infrastructure, which explicitly exploits features of the wireless domain to create a highly secure channel through an otherwise not trustworthy environment. The limited capabilities of small wireless (sensor) devices, such as computational and battery power or the physical access protection of cryptographic keys, can become and obstacle for using advanced cryptography. So, we are after slim and computationally cheap protocols.

Fortunately, some features of wireless networks can be used in order to construct a highly secure transmission channel. Devices are usually simple and small, so it can be very challenging for an adversary to physically locate them in an environment. Such devices are often also cheap and can be deployed in large numbers, thus facilitating the use of secret sharing and/or multi-path transmission.

Intuitively, if we can not make the transmission secure, why not try to make it "invisible"? This it the road taken in the recent paper of (Klonowski et al., 2011), and our goal in this work is further exploring that direction by devising an extended version of their protocol, hereafter referred to as BasicSWTP. We refer the reader to (Klonowski et al., 2011) for full details, and will give only a brief review in section 2.

Organization of the Paper. Preliminaries and groundwork preparation done in Section 2. Section 3 is devoted to a presentation of BasicSWTP and its extension, along with security proofs. Conclusions follow in Section 4.

Related and Previous Work. A lot of papers discuss secret message transmission in wireless networks based on symmetric cryptography and key predistribution (e.g. (Perrig et al., 2004; Jaworski et al., 2009; Cichoń et al., 2009; Anderson et al., 2004; Chan et al., 2003; Du et al., 2005)). The main goal of these protocols is establishing secure channels between devices, where channels are secured by symmetric cryptography. While key management and predistribution Although our scheme can (and should) be used with key-predistribution schemes (Klonowski et al., 2007; Ren et al., 2006), the problem stated in this paper cannot be solved by symmetric schemes with key-predistribution only. Nevertheless, the results in (Chan and Perrig, 2005; Eschenauer and Gligor, 2002) are notable and related and are an asset to our work. Most closely related to ours is the work of (Di Pietro et al., 2006). Our contribution targets the same goals, yet in addition comes with an information-theoretic analysis, which is not provided in previous related work.

Rass S. and Koza M..
On Secure Communication over Wireless Sensor Networks.
DOI: 10.5220/0004018403640367
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 364-367
ISBN: 978-989-8565-24-2

2 PRELIMINARIES

Our network model is the same as in (Klonowski et al., 2011), which is a wireless multi-hop sensor network. In graph-theory language, the network model graph $G(V,E)$ is undirected and t-partite. The (pairwise disjoint) partition $V = L_0 \dot{\cup} L_1 \dot{\cup} \ldots \dot{\cup} L_{t-1}$ is such that no two nodes within the same *layer* L_i talk to each other, and every node from L_i has a logical link (i.e. a symmetrically encrpted channel) to every node in L_{i+1} for $i = 0,1,\ldots,t-2$. One way of building such a layered architecture is using one of many existing clustering protocols (see (Yu and Chong, 2005)) or general key-distribution protocols (e.g. Diffie-Hellman or (Perrig et al., 2004)). We assume low level protocol services like cluster level routing, collision avoidance etc., as provided by the network.

The Basic Transmission Protocol BasicSWTP. On each layer L_i the message m appears split into l parts, which are created by the sender $s \in L_0$ using XOR-secret-sharing. A relay node in L_i ($i \geq 1$) takes its l incoming share parts, combines them to get its message share s_i, invokes another sharing on it and forwards the new parts to l nodes in L_{i+1}. The crux of (Klonowski et al., 2011)'s construction is a special indexing scheme that pseudorandomly determines the receivers in the next layer so that all relay nodes within L_i choose the *same* set of l receivers within L_{i+1}. This assures that the subgraph of G that is used for the actual payload delivery always remains t-partite subgraph, with each intermediate layer having cardinality l. The parameter l controls the number of shares, and hence the number of paths in the transmission, and is called the *forking parameter* (Klonowski et al., 2011). Figure 1 shows an example.

Adversary Model. For security, assume that the adversary corrupts no more than K nodes in total, where a corrupted node has all its content (including any cryptographic keys) exposed to the attacker. Furthermore, we assume the adversary's computational powers sufficiently constrained to inhibit a ciphertext only attack on the symmetric encryption used for any wireless transmission in the network. This assumption is necessary to rule out trivialities by situations in which the adversary gets *all* the information flowing between the sender and the receiver. Notice that this sort of computational intractability assumption might indeed *permit* breaking a public-key encryption.

Security Model. The symbol Π denotes a general message transmission protocol. With $H(\cdot)$ and $H(\cdot|\cdot)$, we denote the unconditional and conditional Shannon-entropy.

Definition 2.1 ((Franklin and Wright, 2000))**.** *Take* $\varepsilon > 0$*, and let* Π *be a message transmission protocol. Suppose that for conveyance of a message* $M \in \{0,1\}^*$*, the packets* $C_1,\ldots,C_n \in \{0,1\}^*$ *are transmitted over the network (constituting the protocol's* transcript*). The adversary's* view *on the transmission of* M *is* $adv(M) \subseteq \{C_1,\ldots,C_n\}$*. A protocol* ε*-secure, if*

- $H(M|adv(M)) \in \{0, H(M)\}$*, and*
- $\mathsf{P}(H(M|adv(M)) = 0) \leq \varepsilon$,

i.e. the adversary can disclose M *with a chance of at most* ε*. We call the protocol* Π efficient*, if the size of the transcript, i.e.* $\sum_{i=1}^{n} |C_i|$*, is polynomial in the size of the message* M*, the size of underlying network (in terms of nodes), and* $\log \frac{1}{\varepsilon}$*. A protocol that is* ε*-secure for any* $\varepsilon > 0$ *is said to enjoy* perfect secrecy.

Security of BasicSWTP. The following two results are found in (Klonowski et al., 2011) and regard the security of the above sketched transmission scheme:

Theorem 2.1. *The strategy of putting all corrupted nodes in exactly one layer maximizes the probability of corrupting the message.*

Corollary 2.2. *In the system with forking parameter* l*, with* n *nodes in each layer, and the adversary capable of corrupting* K *nodes, the probability* p *that the adversary discloses a secret message is*

$$p = \begin{cases} 0, & \text{if } K < l; \\ \binom{K}{l} / \binom{n}{l}, & \text{if } l \leq K < n; \\ 1, & \text{if } K \geq n. \end{cases} \tag{1}$$

The Concept of Vulnerability. For analyzing security, we can set up the transmission as an *attacker-defender-game* in the obvious way: the defender (message *sender*) chooses the t-partite subgraph of G for transmission (grayish nodes in figure 1), while the attacker chooses his nodes to conquer. The game's objective is secret content delivery, so the sender (player 1) scores 1 every securely delivered message, and receives zero payoff in case of a successful message disclosure by the attacker (player 2). The game is zero-sum, meaning that the attacker scores 1 for every disclosed message and zero otherwise. With this setting, standard techniques of game-theory let us determine the optimal behavior for both players, with the optimal strategies of the attacker being characterized by theorem 2.1 already. The optimal revenue for player 1, i.e. the average success-rate of secret messages delivered under the hypothesis that the attacker acts optimal too is the game's saddle-point value v. See (Rass and Schartner, 2010) for full details on this game-theoretic approach. The important fact here is that corollary 2.2 and the details in (Klonowski et al.,

2011) already give us the optimal transmission and attack strategies, along with equation (1) providing the game's saddle-point value.

3 SECURE TRANSMISSION

It is evident that choosing a larger forking parameter occupies more of the network and increases the bandwidth demand. Hence, lower values of l are desirable, yet are paid for with less security.

Framework Protocol. Our proposed extension is running BasicSWTP with a small (fixed) forking parameter on a set of shares to the message, rather than on the message as such. Initially, the message m is shared as $m = r_1 \oplus r_2 \oplus \cdots \oplus r_k$ (where $\oplus$ is the bitwise XOR). Each r_i for $i = 1, 2, \ldots, k$ is transmitted using BasicSWTP with an either chosen or prescribed (small) forking parameter l. The reconstruction by the receiver happens in the obvious way. This "framework protocol", sketched in figure 1 as the wrapper around BasicSWTP, is indeed secure and efficient:

Theorem 3.1. *Let the channel be characterized by the number n of nodes per layer and let the protocol work with a fixed forking parameter $l \leq n$. Assume that a sender estimates the threshold of the adversary as $K \leq n$. Then, in the sense of Definition 2.1, arbitrarily secure communication is efficiently possible if and only if $K < n$.*

Proof sketch: Corollary 2.2 gives the likelihood p of secret delivery in a single round, and the XOR-sharing enforces the attacker to catch all shares whenever the message shall be disclosed. So, if $p = 1$, then the chance to catch all shares is 1 and the transmission is insecure. On the contrary, if $p < 1$, then the chance to catch all of the shares decays exponentially fast, so we can choose k large enough to lower this chance below any chosen $\varepsilon > 0$. The bit-complexity is $k \cdot l \cdot |m|$, where $|m|$ is the length of the message. The overall overhead is $O\left(|m| \cdot l \cdot \log \frac{1}{\varepsilon}\right)$, i.e. polynomial. □

Secure Key-exchange. We can dress up our claims in information-theoretic terms too, if we wrap the framework protocol around BasicSWTP, in order to exchange keys with assured entropy. The following is a technical gadget, needed to establish the second of our results, which is theorem 3.3.

Theorem 3.2 ((Rass and Schartner, 2010)). *Let the sender emit secret messages M of entropy $H(M)$, and let C denote the information that the adversary can acquire by eavesdropping. Then the cross-entropy $I(M;C)$, i.e. the amount of information that leaks out the channel satisfies $I(M;C) \leq \rho \cdot H(M)$, where*

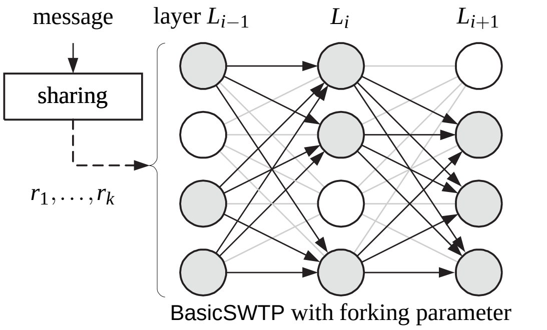
message
layer L_{i-1}
L_i
L_{i+1}
sharing
$r_1, \ldots, r_k$
BasicSWTP with forking parameter
$l = 3$ to convey $r_1, \ldots, r_k$

Figure 1: Example illustration of our protocol.

$\rho = \max \mathrm{P}(successful\ attack)$, and the maximum is taken over all randomized actions of the attacker.

It should be noted that the value ρ in theorem 3.2 can be obtained using game-theoretic tools (Rass and Schartner, 2010) or directly from Corollary 2.2.

Theorem 3.3. *Let a source with entropy h generate a sequence of independent random numbers $r_1, \ldots, r_k$, which are transmitted via BasicSWTP. Let the sender and receiver derive a common secret $\kappa = r_1 \oplus r_2 \oplus \cdots \oplus r_k$. Then, even for a computationally unbounded adversary, the secret has entropy $H(\kappa) \geq (1 - \rho^k)h$, where ρ is given by Corollary 2.2 applied to the instantiation of BasicSWTP.*

Proof sketch: Let the sender transmit k independent uniform random numbers $r_1, \ldots, r_k$ and write $\kappa = r_1 \oplus r_2 \oplus \cdots \oplus r_k$ for the exchanged key κ. By the stochastic independence, the attack probability is by Corollary 2.2 no larger than p^k. Applying Theorem 3.2 with p^k bounds the leaking information $I(C;\kappa) \leq p^k \cdot H(\kappa)$, where C denotes the information that the adversary gains from eavesdropping. By definition, $I(C;\kappa) = H(\kappa) - H(\kappa|C)$, so we get $H(\kappa|C) \geq (1 - p^k) \cdot H(\kappa)$. □

4 CONCLUSIONS

While (Klonowski et al., 2011)'s protocol, here called BasicSWTP, achieves good security based on a free choice of the forking parameter, having multiple such channels run concurrently can quickly occupy and congest the infrastructure. For that matter, it appears reasonable to use another sharing on top of BasicSWTP, which lets us work with smaller forking parameters while not too badly affecting the security (as theorems 3.1 and 3.3 demonstrate).

Our protocol is simple and creates an arbitrary secure channel through a potentially hostile environment. Moreover, it is provably secure and efficient, and does not rest on computational intractability assumptions beyond what is needed to establish secure symmetrically encrypted channels. Even from an information-theoretic point of view, it is possible to use our scheme for secret key-exchange only, so as to gain security even against a computationally unbounded adversary. Moreover, our scheme is lightweight in the sense of imposing little computational effort within each relay node. So it can be implemented in cheap and power-limited devices, particularly small sensor-devices. The protocol offers two degrees of freedom which lets us control the communication overhead and find a suitable balance between security and communication overhead. This facilitates a fair-use policy of the channel, if multiple sessions run concurrently over the same set of devices. In future work, we will report on empirical evaluation via simulation.

Unfortunately, our protocol is vulnerable to denial-of-service attacks in its present form. The XOR-sharing as we used is most vulnerable to corrupted shares, since the secret is unrecoverable if one share is lost or modified. However, XOR-sharing is not a must and might be replaced by conventional polynomial sharing that comes with better error correcting facilities (e.g. Shamir's scheme). Guarding against loss of shares and routing attacks are subject of future research.

This work is written with wireless networks in mind, but the presented algorithm can work in any network where the construction of the aforementioned layered architecture is possible. In particular, it seems possible to apply it in wired networks like cascades of mix servers presented in (Klonowski and Kutylowski, 2005).

ACKNOWLEDGEMENTS

The paper was partially supported by grant S10026 from the Institute of Mathematics and Computer Science of the Wroclaw University of Technology.

REFERENCES

Anderson, R., Chan, H., and Perrig, A. (2004). Key infection: Smart trust for smart dust. In *Proc. of IEEE Int. Conf. on Network Protocols (ICNP)*.

Chan, H. and Perrig, A. (2005). PIKE: peer intermediaries for key establishment in sensor networks. In *INFOCOM 2005. Proc. of the 24th Annual Joint Conf. of the IEEE Computer and Communications Societies.*, volume 1, pages 524–535.

Chan, H., Perrig, A., and Song, D. (2003). Random key predistribution schemes for sensor networks. In *Proc. of the IEEE Symp. on Security and Privacy*, pages 197–213. IEEE Computer Society.

Cichoń, J., Grzaślewicz, J., and Kutyłowski, M. (2009). Key levels and securing key predistribution against node captures. In *ALGOSENSORS*, pages 64–75.

Di Pietro, R., Mancini, L. V., and Mei, A. (2006). Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks. *Wirel. Netw.*, 12:709–721.

Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J., and Khalili, A. (2005). A pairwise key predistribution scheme for wireless sensor networks. *ACM Trans. Inf. Syst. Secur.*, 8(2):228–258.

Eschenauer, L. and Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *CCS '02: Proc. of the 9th ACM Conf. on Computer and communications security*, pages 41–47. ACM Press.

Franklin, M. and Wright, R. (2000). Secure communication in minimal connectivity models. *J. of Cryptology*, 13(1):9–30.

Jaworski, J., Ren, M., and Rybarczyk, K. (2009). Random key predistribution for wireless sensor networks using deployment knowledge. *Computing*, 85(1–2):57–76.

Klonowski, M., Koza, M., and Kutyłowski, M. (2011). How to transmit messages via WSN in a hostile environment. In *Proc. of the Int. Conf. on Security and Cryptography (SECRYPT)*, pages 134–143. SciTePress.

Klonowski, M. and Kutylowski, M. (2005). Provable anonymity for networks of mixes. In *Information Hiding*, pages 26–38.

Klonowski, M., Kutyłowski, M., Ren, M., and Rybarczyk, K. (2007). Forward-secure key evolution in wireless sensor networks. In *CANS*, pages 102–120. Springer.

Perrig, A., Stankovic, J. A., and Wagner, D. (2004). Security in wireless sensor networks. *Commun. ACM*, 47(6):53–57.

Rass, S. and Schartner, P. (2010). A unified framework for the analysis of availability, reliability and security, with applications to quantum networks. *IEEE Trans. on Systems, Man, and Cybernetics – Part C: Applications and Reviews*, 40(5):107–119.

Ren, M., Das, T. K., and Zhou, J. (2006). Diverging keys in wireless sensor networks. In *ISC*, pages 257–269.

Yu, J. Y. and Chong, P. H. J. (2005). A survey of clustering schemes for mobile ad hoc networks. *Communications*, 7(1):32–48.