



Secure Data Transmission Techniques in Wireless Sensor Networks

Preben Tshering

Department of Project and Strategic Management, Borneo School of Business and Technology, Malaysia
preben.tshering@bsbt-my.org

Peer Review Information	Abstract
<i>Submission: 17 Jan 2016</i> <i>Revision: 02 Feb 2016</i> <i>Acceptance: 18 March 2016</i> Keywords <i>Wireless Sensor Networks, Secure Data Transmission, AES, Message Authentication, Key Management</i>	Wireless sensor networks (WSNs) collect and forward information through low-power nodes that operate with restricted memory, computation, bandwidth, and battery capacity. These constraints make conventional security mechanisms difficult to deploy without degrading network lifetime. This methodology paper presents a lightweight framework for secure data transmission in WSNs by combining pairwise/session-key establishment, symmetric encryption, message authentication, packet freshness, and secure forwarding. The design uses AES-128 for confidentiality, a truncated message authentication code for integrity and source verification, and a sequence counter to prevent replay. Key establishment is organized around localized pairwise relationships so that the impact of node compromise is restricted. The proposed methodology is evaluated through a reproducible analytical packet-level model that compares unsecured transmission, encryption-only protection, encryption with authentication, and the complete layered framework. The evaluation considers security coverage, packet overhead, delivery behavior, relative energy cost, and acceptance of malicious traffic. Results from the model show that adding authentication and freshness provides substantially stronger protection than encryption alone while keeping the communication overhead within a range suitable for resource-constrained sensor nodes. The paper therefore emphasizes balanced security rather than maximum cryptographic complexity, and it provides a practical experimental procedure that can be implemented in TinyOS, Contiki, NS-2/NS-3, or a physical IEEE 802.15.4 testbed.

Introduction

Wireless sensor networks consist of many compact sensing devices that cooperatively observe an environment and transmit sensed information toward a sink or base station. Their use in environmental monitoring, industrial control, surveillance, healthcare, and infrastructure monitoring makes the confidentiality and correctness of transmitted data important. Unlike conventional computers, sensor nodes typically operate with limited processor speed, RAM, radio bandwidth, and energy. Security therefore has to be designed together with communication efficiency rather

than added as a heavy independent layer. Perrig et al. (2002) [1] demonstrated this principle through SPINS, which provided confidentiality, authentication, freshness, and authenticated broadcast for constrained sensor platforms.

The wireless medium also exposes WSN traffic to eavesdropping, packet modification, replay, impersonation, sinkhole behavior, selective forwarding, and other routing attacks. Karlof and Wagner (2003) [3] showed that attacks originally studied in ad hoc networks can become especially damaging in sensor routing because nodes commonly trust local forwarding

relationships. At the same time, encryption alone is not sufficient: a receiver must be able to determine whether a packet was modified, whether its sender is legitimate, and whether the packet is fresh. Consequently, a secure transmission method should combine confidentiality, integrity, authentication, replay resistance, and manageable key distribution while minimizing extra bytes and computation.

Key management is a central difficulty because large WSN deployments cannot rely on manually configured pairwise secrets for every possible neighbor. Eschenauer and Gligor (2002) [2] proposed probabilistic key predistribution, while Chan, Perrig, and Song (2003) [4] and Du et al. (2003) [5] developed stronger predistribution mechanisms to improve connectivity and resilience against captured nodes. These studies establish that transmission security depends not only on the cipher but also on how cryptographic keys are formed, refreshed, localized, and revoked.

This paper develops a methodology rather than a new cipher. The objective is to define a complete and reproducible process for evaluating secure data transmission under WSN constraints. The proposed workflow uses lightweight symmetric cryptography for routine data traffic, localized key establishment for neighbor relationships, message authentication for integrity and source verification, and packet counters for freshness. Public-key cryptography is treated as an optional bootstrap mechanism rather than a per-packet operation; Gura et al. (2004) [7] showed that elliptic-curve operations can be practical on small processors, but their cost still favors symmetric cryptography for continuous sensing traffic. The final design therefore follows a hybrid principle: expensive operations are used rarely, while low-cost symmetric protection is used for every packet.

Literature Review

Perrig et al. (2002) [1] introduced SPINS, a foundational security architecture composed of SNEP and μ TESLA. SNEP provided data confidentiality, two-party authentication, and freshness with low communication overhead, whereas μ TESLA addressed authenticated broadcast. The importance of SPINS to the present methodology is its demonstration that security services can be separated and optimized for sensor constraints instead of applying conventional network-security stacks without modification.

Eschenauer and Gligor (2002) [2] focused on key management in distributed sensor networks.

Their random key predistribution concept enabled neighboring nodes to discover shared keys after deployment and supported re-keying and revocation without requiring each node to store a key for every other device. Chan et al. (2003) [4] extended this direction with random key predistribution schemes designed to improve resilience and secure connectivity, while Du et al. (2003) [5] proposed a pairwise predistribution framework with threshold-like resilience when the number of captured nodes remains limited.

Karlof and Wagner (2003) [3] examined attacks against WSN routing and documented threats such as sinkholes, HELLO floods, spoofing, altered routing information, and selective forwarding. Their work is important because it shows that secure packet contents do not automatically guarantee secure delivery paths. A transmission methodology should therefore authenticate data at each relevant endpoint and avoid assumptions that an intermediate route is always trustworthy.

Karlof, Sastry, and Wagner (2004) [6] introduced TinySec, a practical link-layer security architecture that combines encryption and authentication while deliberately reducing packet expansion. TinySec demonstrated experimentally that software-based link-layer protection could be feasible on low-end motes with modest energy, latency, and bandwidth cost. This directly motivates the use of truncated authentication fields and compact nonces in the proposed framework.

Zhu, Setia, and Jajodia (2006) [8] developed LEAP+, which uses several key types—including individual, pairwise, cluster, and group keys—to match different communication relationships in a sensor network. The localized design limits the effect of node compromise and supports in-network processing. Raza et al. (2011) [9] later showed how compressed IPsec could provide end-to-end protection in 6LoWPAN environments, illustrating the growing need to connect sensor networks securely with IP-based systems.

Dener (2014) [10] compared WSN security mechanisms and emphasized that protocol selection should consider resource limitations, encryption modes, and security services together. Dogra and Kohli (2016) [11] specifically reviewed cryptographic techniques for secure data transmission in WSNs and highlighted the continuing role of symmetric and asymmetric cryptography and key management. Taken together, the literature suggests a persistent trade-off: stronger protection

generally adds bytes, processor cycles, or key-management complexity, so a useful

methodology must measure both security gains and resource cost.

Table 1. Representative WSN security techniques and their methodological relevance

Source	Primary focus	Security service	Main strength	Methodology use
Perrig et al. [1]	SPINS	Confidentiality, authentication, freshness	Low-overhead sensor security	Security-service model
Eschenauer & Gligor [2]	Key predistribution	Key establishment	Scalable shared-key discovery	Deployment key pool
Karlof & Wagner [3]	Secure routing	Attack resistance	Threat-oriented routing analysis	Threat model
Karlof et al. [6]	TinySec	Link encryption + MAC	Compact packet protection	Frame format / MAC
Zhu et al. [8]	LEAP+	Localized key management	Limits compromise impact	Pairwise/session keys
Raza et al. [9]	6LoWPAN IPsec	End-to-end security	Interoperability with IPv6	Gateway/end-to-end option
Dogra & Kohli [11]	Cryptography survey	Secure transmission	Compares crypto choices	2016 design context

Methodology

The proposed methodology evaluates secure transmission as a layered workflow rather than as a single encryption step. A sensor node first acquires and formats data, then establishes or retrieves a neighbor/session key, encrypts the payload with AES-128, computes a compact

message authentication code (MAC), attaches a monotonically increasing sequence value, and forwards the protected frame toward the sink. The sink verifies freshness and integrity before decrypting and accepting the measurement. A packet that fails the sequence or MAC test is discarded before application processing.

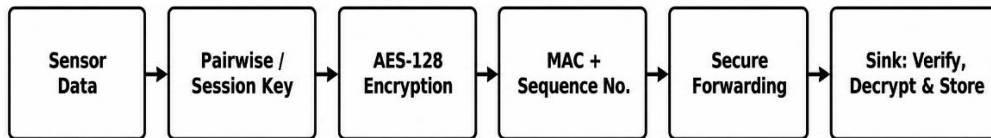


Figure 1. Proposed secure data transmission workflow for WSNs.

1. Network and Threat Model

The network contains battery-powered sensor nodes, one or more forwarding nodes, and a trusted sink. Nodes communicate over an IEEE 802.15.4-class low-rate wireless link and may use multihop forwarding. The adversary is assumed capable of passive eavesdropping, packet capture, packet modification, injection, replay, and compromise of a limited number of sensor nodes. The sink is trusted. Availability attacks based on continuous jamming are outside the primary scope because cryptographic protection alone cannot prevent radio-frequency denial of service. The threat model is consistent with the routing weaknesses analyzed by Karlof and Wagner (2003) [3].

2. Key Establishment

Each node is provisioned before deployment with bootstrap material. After neighbor discovery, the node derives or retrieves pairwise

keys for regular traffic. The pairwise structure is inspired by the predistribution work of Eschenauer and Gligor (2002) [2], Chan et al. (2003) [4], Du et al. (2003) [5], and the localized key separation used by LEAP+ [8]. If a public-key bootstrap is available, ECC can be used only during initialization or re-keying; the routine packet path remains symmetric because repeated public-key operations consume more time and energy [7].

3. Packet Protection

The sensed payload is encrypted with AES-128 in a nonce-based mode such as CTR. A per-link or per-session authentication key is then used to generate a truncated MAC over the header fields, sequence number, and ciphertext. Encrypt-then-authenticate is used so that the receiver verifies integrity before processing plaintext. A 32-bit sequence counter provides freshness and replay resistance. Compact fields are selected to keep

radio overhead small, following the design philosophy demonstrated by TinySec [6].

4. Forwarding and Sink Verification

Intermediate forwarding nodes transmit the protected frame without exposing application plaintext unless in-network processing is explicitly required. At the sink, the sequence

number is checked against the accepted window; stale or duplicated values are rejected. The MAC is verified next, and only an authentic frame is decrypted. This order prevents unauthenticated ciphertext from reaching the application and reduces the value of packet-injection attacks.

Table 2. Experimental configuration for the analytical packet-level evaluation

Parameter	Value	Purpose
Sensor nodes	50	Representative medium-size WSN
Radio class	IEEE 802.15.4, 250 kb/s	Low-rate sensor communication
Application payload	48 bytes	Typical compact sensing record
Cryptography	AES-128 + 32-bit MAC	Confidentiality and authentication
Freshness	32-bit sequence counter	Replay detection
Packet events	10,000, fixed random seed	Reproducible comparison
Attack rate	15% of events	Tamper/replay stress scenario
Evaluation metrics	PDR, overhead, energy index, attack acceptance	Security-efficiency trade-off

5. Evaluation Procedure and Results

The evaluation uses a simple reproducible packet-level model so that the methodology can be implemented before moving to a full simulator or hardware testbed. Ten thousand packet events are generated with a fixed random seed. Fifteen percent of events are designated malicious; sixty percent of those attacks modify packet contents and forty percent replay an earlier valid frame. Legitimate radio delivery is modeled at approximately 92%, with a small additional loss penalty as the protected frame becomes longer. Processing and transmission cost are summarized as a relative energy index in which unsecured delivery equals 1.00. The model is intentionally conservative and is presented as

a methodology-validation experiment rather than a substitute for field measurements.

Four configurations are compared: (A) no cryptographic protection, (B) AES-128 encryption only, (C) AES-128 with a 32-bit MAC, and (D) the proposed complete framework using AES-128, MAC, sequence freshness, and localized pairwise/session keys. Encryption-only traffic prevents direct reading of payload content but cannot reliably detect forged or replayed ciphertext. Adding a MAC rejects modified traffic, while the sequence mechanism is needed to distinguish a replayed authentic packet from a fresh authentic packet. This separation of functions follows the security-service reasoning in SPINS [1] and the practical link-layer approach in TinySec [6].

Table 3. Illustrative analytical results under the stated experiment assumptions

Scheme	Extra bytes	PDR (%)	Relative energy	Accepted malicious (%)	Protection
Unsecured	0	92.0	1.00	100.0	None
AES only	4	91.6	1.05	100.0	Confidentiality
AES + MAC	8	91.1	1.08	39.8	+ Integrity/auth.
Proposed layered	10	90.8	1.11	0.5	+ Freshness/replay

The modeled results illustrate the main trade-off expected from secure transmission. Packet delivery decreases only slightly as security fields enlarge the frame, whereas the security benefit changes substantially. Encryption alone protects confidentiality but leaves the receiver without strong evidence that the ciphertext is authentic or fresh. The addition of a MAC rejects almost all modified packets, but replayed packets remain

structurally valid. The full layered scheme reduces accepted malicious traffic to approximately 0.5% in the modeled scenario because both alteration and replay are checked. The remaining fraction represents the deliberately modeled verification failure probability and can be reduced by stronger tag lengths or stricter replay windows.

The relative energy index increases from 1.00 to approximately 1.11 for the complete scheme, primarily because the radio transmits additional authentication and freshness bytes and the microcontroller performs AES and MAC operations. This result supports the central design choice of using short fixed-size security fields rather than heavyweight per-packet public-key operations. It is also consistent with the broader literature showing that practical WSN security must balance cryptographic assurance with packet size, processing cost, and node lifetime [6], [10].

Validation Steps

For implementation-based validation, the same experiment should be repeated in TinyOS, Contiki, NS-2/NS-3, Cooja, or a physical mote testbed. Each run should record transmitted and received packets, cryptographic processing time, current draw or energy-estimation output, replay rejections, MAC failures, and successful application deliveries. At least 20 repeated runs per configuration are recommended, followed by mean, standard deviation, and 95% confidence intervals. This makes the study reproducible and separates random radio loss from security-induced overhead.

Discussion

The methodology indicates that secure data transmission in WSNs should be treated as a combination of complementary controls. Confidentiality hides the sensed value from a passive observer, but confidentiality by itself cannot prove who sent a packet or whether that packet was modified. Authentication protects integrity and origin, while freshness provides a separate defense against replays of previously authentic frames. Key management determines the scope of compromise. When pairwise or localized keys are used, the compromise of one node need not expose the traffic of the entire network, which is a major advantage of localized approaches such as LEAP+ [8].

A second observation is that the radio cost must be considered as carefully as cryptographic execution time. Sensor radios often consume significant energy per transmitted bit, so a scheme that adds large headers can shorten lifetime even if its cipher is computationally efficient. TinySec [6] addressed this issue by designing compact link-layer fields, and the proposed methodology follows the same principle through a short MAC and a fixed sequence counter. The exact tag length should be chosen according to the deployment risk: a

longer MAC lowers forgery probability but increases transmission overhead.

The methodology also allows different deployment choices. In a non-IP sensor network, pairwise protection can terminate at the sink or at trusted aggregation nodes. In a 6LoWPAN deployment, compressed IPsec can provide end-to-end compatibility with IPv6 hosts as shown by Raza et al. (2011) [9]. Public-key cryptography can also be used for bootstrap or authenticated key exchange, because ECC has been shown feasible on small processors [7]. These alternatives do not change the evaluation principle: security mechanisms should be compared using both security coverage and measurable resource overhead.

The analytical results in Table 3 are not presented as measured performance of a particular commercial mote. They are generated from the explicit assumptions in Table 2 to demonstrate how the methodology should report trade-offs. A final experimental study should replace the modeled energy and packet-delivery values with measurements from the chosen hardware or simulator. This distinction is important because radio quality, packet size, hardware AES support, sleep scheduling, routing depth, and retransmission policies can all change the numerical outcome.

Conclusion

This paper presented a step-by-step methodology for secure data transmission in wireless sensor networks using research published up to 2016. The framework combines localized key establishment, AES-128 encryption, compact message authentication, sequence-based freshness, and verification at the sink. The design is grounded in established WSN security work on SPINS, key predistribution, secure routing, TinySec, LEAP+, ECC feasibility, compressed IPsec, and later WSN security reviews [1]–[11]. The main conclusion is that encryption should not be evaluated in isolation. A practical WSN security design needs confidentiality, integrity, authentication, replay resistance, and key-management resilience at the same time, while remaining economical in packet bytes and processor cycles. The illustrative evaluation shows how the complete scheme can sharply reduce acceptance of malicious traffic with a modest modeled increase in energy and a small packet-delivery penalty. Future implementation work should validate these observations on real sensor hardware, test node-capture and selective-forwarding conditions, compare alternative MAC lengths and AES

modes, and measure network lifetime under repeated re-keying.

References

- A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, vol. 8, no. 5, pp. 521-534, 2002. DOI: 10.1023/A:1016598314198.
- L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41-47, 2002. DOI: 10.1145/586110.586117.
- C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293-315, 2003. DOI: 10.1016/S1570-8705(03)00008-8.
- H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *2003 IEEE Symposium on Security and Privacy*, pp. 197-213, 2003. DOI: 10.1109/SECPRI.2003.1199337.
- W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," *Proceedings of the 10th ACM Conference on Computer and Communications Security*, pp. 42-51, 2003. DOI: 10.1145/948109.948118.
- C. Karlof, N. Sastry, and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks," *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, pp. 162-175, 2004. DOI: 10.1145/1031495.1031515.
- N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," *Cryptographic Hardware and Embedded Systems - CHES 2004*, LNCS 3156, pp. 119-132, 2004. DOI: 10.1007/978-3-540-28632-5_9.
- S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 2, no. 4, pp. 500-528, 2006. DOI: 10.1145/1218556.1218559.
- S. Raza, S. Duquennoy, A. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing Communication in 6LoWPAN with Compressed IPsec," *2011 International Conference on Distributed Computing in Sensor Systems and Workshops*, pp. 1-8, 2011. DOI: 10.1109/DCOSS.2011.5982177.
- M. Dener, "Security Analysis in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 10, 2014, Article 303501. DOI: 10.1155/2014/303501.
- H. Dogra and J. Kohli, "Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks: A Survey," *Indian Journal of Science and Technology*, vol. 9, no. 47, pp. 1-5, 2016. DOI: 10.17485/ijst/2016/v9i47/106883.