ISSN 2278-9723
doi: 10.31838/ijccts/07.01.05

Research Article

ENHANCEMENT OF SECURITY AND NETWORK LIFETIME USING FLEXI CAST METHOD

[1]SARANYA.U, [2]MADHUBALA.P
[1]PG scholar/CSE, Tagore Institute of Engineering and Technology, Salem, India.
[2]Assistant Professor/CSE, Tagore Institute of Engineering and Technology, Salem, India.
Email id :saranya.u@gmail.com[1].
Received:08 .02.19, Revised: 11.06.19, Accepted:05.08.19

ABSTRACT
Sensor nodes can reprogram themselves using software objects broadcast by a base station. Sensor nodes can efficiently detect a modification in software objects sent by a base station or stored in neighboring nodes through authenticated fingerprints and network-wide attestation. The Proposed analysis shows that Flexi Cast can reduce energy consumption for both updating software objects and checking modifications regarding more critical attack.

Keywords: Flexicast

INTRODUCTION

A recurring problem of the TESLA approaches is the denial of service attacks. As a result of its delayed authentication feature, unauthenticated messages need to wait for the key disclosure to happen in the following interval. They fill up the available buffer of sensor nodes and the DoS attackers try to deplete the buffer by sending arbitrary packets to targets. The target sensor nodes become more vulnerable to the DoS attack as it stores more unauthenticated packets for an interval. Moreover, in WASNs, a large software object generates bursty traffic in which a number of packets are delivered in a single interval, which decreases the resilience against the DoS attack. The security of the ShortPK approaches is tuned for energy efficiency. public key cryptography still consumes far more energy compared with hash operations of TESLA; an 80-bit ECDSA operation uses 36 times more energy than a SHA-1 operation. The ShortPK approaches are not suitable for authenticating a number of packets of a large software object.

Literature Survey

Energy Budget Analysis for Signature Protocols on a Self-powered Wireless Sensor Node(Krishna Pabbuleti, Deepak Mane and Patrick Schaumont,(2014) [1]. The Internet of Things will include many resource constrained wireless sensing devices, hungry for energy, bandwidth and compute cycles. The sheer amount of devices involved will require new solutions to handle issues such as such as identification and power provisioning. In this contribution, they analyze the energy needs of several public key based authentication protocols, taking into account the energy cost of communication as well as of computation. To built an autonomous energy harvesting sensor node which
includes a micro controller RF unit, and energy harvester. The investigation of the Elliptic Curve Digital Signature Algorithm (ECDSA), the Lamport

Die one time hash based Signature scheme(LDOTS) and the Winternitz one time hash based signature scheme(WTS). To demonstrate that there's a trade between energy used for communication, energy used for computaion, and security level, consider the energy needs for the over all system, we show that all schemes are within one order of magnitude from each another. Preparation.

A new key establishment scheme for wireless sensor networks (Eric Ki Wang, Lucas C.K.Hui and S.M.Yiu,(2009)[2]. Traditional key management techniques, such as public key cryptography or key distribution center are often not effective for wireless sensor networks for the serious limitations in terms of computational power energy supply, network bandwidth. In order to balance the security and efficiency, they proposed a new scheme by employing LU Composition techniques for mutual authenticated pairwise key establishment and integrating LU Matrix with Elliptic Curve Daffy Hellman for anonymous path key establishment. It is able to achieve efficient group key agreement and management. Analysis that the new scheme has better performance and provides authenticity and

anonymity for sensor to establish multiple kinds of keys, compared with previous related works.

Efficient reprogramming of wireless sensor networks using incremental updates and data compression (Milosz Stoic, Pieter J. L. Chippers, Johan J. Lucien,(2012)[3]. Reprogramming is an important issue in wireless sensor networks. It enables to extend or correct functionality of a sensor network after deployment, at a low cost. In this paper we, investigate two problems: improving the energy e_ciency and improving the delay of programming. As enabling technologies we use data compression and incremental updates. We analyze deferent algorithms for both approaches, as well as their combination, when applied to resource-constrained devices. All algorithms are ported to the Contac embedded operating system, and prowled for deferent types of reprogramming. Our results show that there is a clear trade-o_ between performance and resource requirements. Either VCDIFF, or the combination of Lempel-Ziv-77 or Fast compression to other compression algorithms.

Proposed Work

A new energy-efficient method called Flexi Cast to perform both authenticated broadcast and software attestation in IWASNs. In Flexi Cast, active sensor nodes can efficiently check the integrity of software objects of their own and neighbor sensor nodes. Efficient, secure delivery via authenticated fingerprints: In the authenticated fingerprinting, before sending a large software object, a base station generates fingerprints, which are managed Bloom filters of the software objects, and delivers the fingerprints securely. Using the fingerprints, sensor nodes can efficiently check the integrity of packets followed by the fingerprints. Coordinated network-wide software attestation for non-identical sensor nodes: In FlexiCast, a base station coordinates network-wide attestation to detect software modification on every node efficiently. The base station initiates the software attestation phase with a new challenge. Since the challenge is common, each sensor node calculates the checksum once but its answers are unique through hashing them with nonces from neighbor nodes. The base station reveals the correct answers after exchanging answers among neighbor nodes and sensor nodes can validate neighbor nodes. Semantic-aware, prioritized checksum for efficient attestation: It is hard to achieve full-coverage checksum In FlexiCast, a base station builds a control slot map containing an encoded list of the addresses of control transfer instructions to avoid the extra scan steps.

Proposed Algorithm

1. Software object to be broadcast and creates a control slot map that is appended to the image. 2. Control slot map in Second, the base station splits the image into packet-size chunks and creates a Bloom filter on the chunks. Since the generated Bloom filter represents the unique features of the image, we can use it asa fingerprint.3. Base station broadcasts the fingerprint before sending the packets of the software object. Since sensor nodes should be able to trust the fingerprint, the base station delivers it via a broadcast authentication scheme and then waits until all of the sensor nodes authenticate the fingerprint. For example, the base station waits for key disclosure if TESLA is used or waits for the delivery time to the furthest sensor node plus the verification time if ShortPK is used. After ensuring that the fingerprint is authenticated, the base station starts to broadcast the packets. When receiving the packets, a sensor node simply performs the membership check of the Bloom filter on the received packet.

Figure 1: Flexicast

Procedure

Input:

A software object Q, the size of maximum payload M, and the lower bound of false positive p for fingerprints
Scan Q and generate the control slot map C
Append C to Q
Split Q||C into packets
foreach Q do
foreach hach function, h() do
set b by h(Q)
end
calculate the probability of false positive p of b
if p>P then
b>F
end
end
foreach b&F do
Broadcast the authenticated form of b
end
waiting all b are authenticated
foreach Q do
Broadcast Q
end

Experimental Results

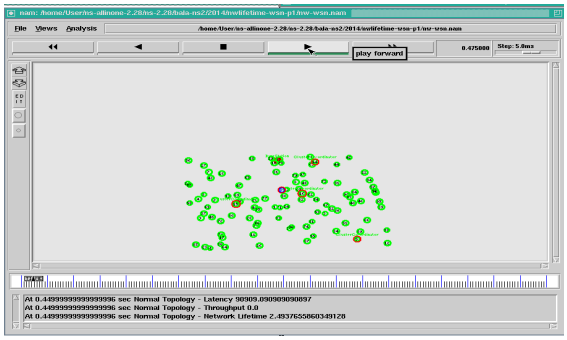

Figure 2: Node simulation

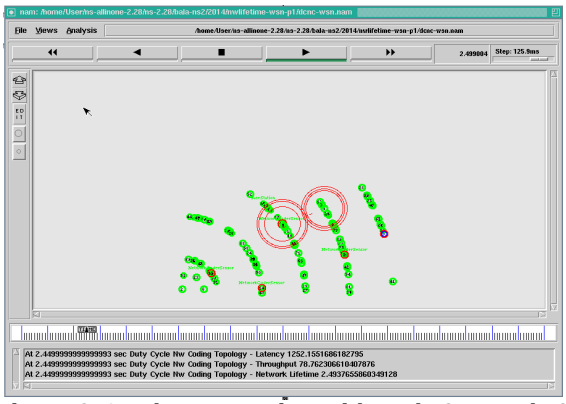

Figure 3: Sends Data Packet with node 9 to Node 6

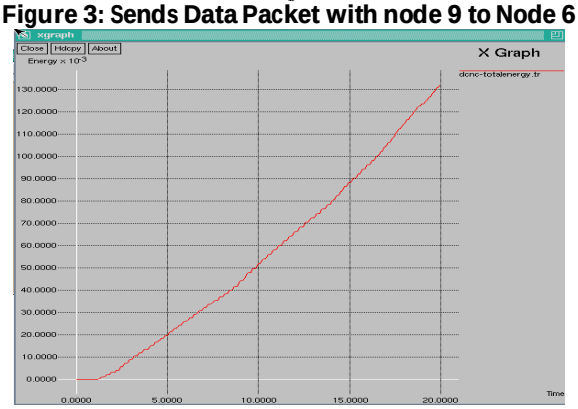

Figure 4: Graphical representation

Conclusion

Previous schemes for security are inefficient for energy consumption in IWASNs because they do not care about the use of software objects. Without energy restriction, security can be guaranteed in a number of ways. However, in the real world, It should be able to provide the best security under conditions of limited energy and operations. Proposed FlexiCast for energy-limited sensor nodes to check the integrity of software objects. The base station controls the authenticated fingerprinting and network-wide attestation to build a trust base on software objects and energy-limited sensor nodes benefit from the efficiency of FlexiCast.

References

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey,"Computer Networks, vol. 38, no. 4, pp. 393– 422, 2002.
2. J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.
3. C. F. Hsin and M. Liu, "Randomly duty-cycled wireless sensor networks: dynamic of coverage,"IEEE Trans. Wireless Commun.,vol.5,no.11, pp. 3182–3192, 2006.
4. X. Y. Wang, R. K. Dokania, and A. Apsel, "PCO-based synchronization for cognitive duty-cycled impulse radio sensor networks,"IEEE Sensors J., vol. 11, no. 3, pp. 555–563, 2011.
5. Q. Wang and T. Zhang, "Bottleneck zone analysis in energy-constrained wireless sensor networks,"IEEE Commun. Lett., vol. 13, no. 6, pp. 423– 425, June 2009.
6. D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," ACM SIGMOBILE Mobile Computing and Commun. Rev., vol. 5, no. 4, pp. 11–25, 2001.
7. R. Ahlswede, N. Cai, S. Y. R. Li, and R. Yeung, "Network information flow,"IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, July 2000.
8. O. M. Al-Kofahi and A. E. Kamal, "Network coding-based protection of many-to-one wireless flows,"IEEE J. Sel. Areas Commun.,vol. 27, no. 5, pp. 797–813, 2009.
9. S.-Y. Li, R. W. Yeung, and N. Cai, "Linear network coding," IEEE Trans. Inf. Theory, vol. 49, no. 2, pp. 371–381, 2003.
10. S. Lee and S. H. Lee, "Analysis of network lifetime in cluster-based sensor networks," IEEE Commun. Lett., vol. 14, no. 10, pp. 900–902, 2010.
11. M. Bhardwaj, T. Garnett, and A. Chandrakasan, "Upper bounds on the lifetime of sensor networks," in Proc. 2001 IEEE ICC, pp. 785–790.
12. H. Zhang and J. C. Hou, "On the upper bound ofα−lifetime for large sensor networks," ACMTrans.Sen.Netw., vol. 1, no. 2, pp. 272–300,2005.
13. D. Liu and P. Ning, "Multilevel _TESLA: Broadcast authentication for distributed sensor networks," Trans. on Embedded Computing Sys.,vol. 3, no. 4, pp. 800–836, 2004.
14. J. Tian, G. Wang, T. Yan, and W. Zhang, "A Power-Efficient Scheme for Securing Multicast in Hierarchical Sensor Networks," in ICCCN '09: Proceedings of the 18th Internatonal Conference on Computer Communications and Networks. IEEE, 2009, pp. 1–6.
15. L. You and L. Yang, "An improved short-term public key-based broadcast authentication in wireless sensor networks," in CIICT '02:Proceedings of Symposium on ICT and Energy Efficiency and Workshop on Information Theory and Security, 2012, pp. 28–34.

16. A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla, "Pioneer: verifying code integrity and enforcing untampered code execution on legacy systems," ACM SIGOPS Operating Systems Review, vol. 39, no. 5, pp. 1–16, 2005.
17. S. Kiyomoto and Y. Miyake, "Lightweight Attestation Scheme for Wireless Sensor Network." International Journal of Security & Its Applications, 2014.
18. I.-R. Chen and Y. Wang, "Reliability Analysis of Wireless Sensor Networks with Distributed Code Attestation," IEEE Commun. Lett., vol. 16, no. 10, pp. 1640–1643, Oct. 2012.
19. S. K. Cha, B. Pak, D. Brumley, and R. J. Lipton, "Platform-independent programs," in CCS '10: Proceedings of the 17th ACM conference on Computer and communications security. New York, New York, USA: ACM Request Permissions, Oct. 2010, pp. 547–558.
20. B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of ACM, vol. 13, pp. 422–426, 1970.
21. K. Pabbuleti, D. Mane, and P. Schaumont, "Energy Budget Analysis for Signature Protocols on a Self-powered Wireless Sensor Node," in RFIDsec '14: Proceedings of the 10th Workshop on RFID Security, May 2014, pp. 1–14.
22. M. Mitzenmacher and E. Upfal, Probability and computing: Randomized algorithms and probabilistic analysis. Cambridge University Press,2005.