International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Secure Mechanism for Wireless Sensor Networks

Tabbasum Sajjan Magdum[1], Y.B.Gurav[2]

[1]Pune University, Padmbhooshan Vasantdada Patil Institute of Engineering & Technology, Pune, Maharashtra, India

[2]Professor, Pune University Padmbhooshan Vasantdada Patil Institute of Engineering & Technology, Pune, Maharashtra, India

Abstract: ***As Wireless Sensor Networks are proceeding towards wide-spread deployment, security issues become a central issue. Assuring the security of communication and access control in Wireless Sensor Networks (WSNs) has huge importance. So far, huge research has focused on making Wireless Sensor Networks feasible and useful, and has not concentrated on security. A security technique, MoteSec-Aware, is presented based on the network layer for WSNs with concentrate on secure network protocol and data access control. For identifying the replay and jamming attacks focused around the symmetric key cryptography utilizing AES as a part of OCB mode, a Virtual Counter Manager (VCM) with a synchronized incremental counter is introduced in the secure network protocol of MoteSec-Aware. The Key-Lock Matching (KLM) system to stop unauthorized access is investigated for access control. MoteSec-Aware is built for the TelosB model sensor platform running TinyOS 1.1.15, and conduct field tests and TOSSIM-based simulations to assess the performance of MoteSec-Aware. The results show that MoteSec-Aware expends substantially less energy, yet accomplishes higher security levels than a number of state-of-the-art techniques.***

Keywords: Wireless Sensor Networks, Security, Replay attacks, Jamming attacks.

1. Introduction

A Wireless Sensor Network (WSN) is typically made up of a number of resource-limited sensor nodes, which can work synergistically and distribute helpful data to user on their queries and events. Wireless Sensor Networks are heterogeneous frameworks consist of a number of small devices known as sensor nodes and actuators with universally useful computing components. These networks will comprise a huge number of low cost, low power and self-organizing nodes that are extremely distributed either inside the framework or close it. The WSN is manufactured of "nodes" ranging from a few to several, where every node is associated with one or many sensors. These nodes comprise of three principle segments data processing, sensing and communication. Two different components are additionally there known as, aggregation and base station. Aggregation point's collects data from their different neighboring nodes and combines the collected data and after that forwards it to the base station for processing. There are different applications of WSN such as military applications, ocean and wildlife monitoring, environmental observation, forecast systems and different sorts of intelligent systems.

The most of existing systems are bi-directional, likewise empowering control of sensor movement. The advancement of wireless sensor systems was motivated by military applications, for example, battlefield surveillance; today such systems are utilized as a part of numerous modern and consumer applications for example health monitoring. Generally every wireless sensor network node has a few parts: energy source, typically a battery, a radio transceiver, a microcontroller, an electronic circuit.

Since sensor nodes may gather sensitive data, security and privacy turn into a concern which cannot be disregarded. Also, a number of real-world situations, including group/environment checking, smart home, require information distribute over the network and information stored in nodes' memories. Because of the resource-limited sensor nodes, conventional network security techniques are not suitable for WSNs. Encouraged by the above difficulties; the problem of secure network protocol and information access control in WSNs is studied to prevent data leaking to an unauthorized party. As literature suggests secure mechanisms for wireless sensor networks are not implemented yet.

2. Literature Review

Adrian Perrig et. al [1] have effectively showed the possibility of implementing a security subsystem for a greatly limited sensor network platform. They have distinguished and built valuable security protocols for sensor networks: legitimate and private communication, and legitimate broadcast. To demonstrate the utility of their security building parts, they built an authenticated routing plan and a safe node-to-node key agreement convention. Numerous components of their configuration are universal and apply effectively to other sensor networks. Since their primitives are exclusively focused on fast symmetric cryptography, and utilize no asymmetric algorithms, their building blocks are appropriate to a wide diversity of device configurations. For symmetric cryptography, the computation costs of are very low. Indeed on limited platform the energy used for security is insignificant contrasted with the energy cost of sending or getting messages. Without different constraints, it ought to be conceivable to encrypt and authenticate all sensor readings. The communication costs are little. As the data authentication, freshness, and privacy properties oblige transmitting only 8 bytes for every unit, it is possible to ensure these properties on a for every packet premise, even with little 30 byte packets. It is hard to enhance this plan, as transmitting a MAC is essential for ensuring data authentication.

Certain components of the design were impacted by the experimental platform. The decision of RC5 as their cryptographic primitive falls into this class; on an all the more capable platform they could utilize any number of shared key algorithms to equivalent achievement. The great emphasis on code reuse is an alternate property constrained by their platform. A powerful device would permit more essential modes of authentication. The principle constraint of their platform was available memory. Specifically, the buffering constraint restricted the viable bandwidth of authenticated broadcast. Notwithstanding the inadequacies of their target platform, they had the capacity to show a security subsystem for the model sensor network.

In [2], TinySec attains security in devices where energy and processing power puts critical resource limitations. C. Karlof et. al [2] have implemented TinySec to attain these deficiencies utilizing the lessons they have gained from different security protocols. They have attempted to highlight their configuration process from a cryptographic point of view that meets both the deliberate resource limitations and security prerequisites. TinySec depends on cryptographic primitives that have been confirmed in the security community for a long time. Their TinySec usage is in wide use all through the sensor network community. They know of researchers constructing key exchange protocols on top of TinySec. Others have ported TinySec to their custom equipment. TinySec is sufficiently straightforward to coordinate into existing applications that the load on application software engineers is negligible.

M. Luk et. al [3] have concluded that Battery energy is the primary resource to preserve in present remote sensor networks. Researchers have presented a number of methods for securing communication that improve either for state of security or for low energy usage. Their secure sensor network communication package, MiniSec, offers a high level of security while obliging very less energy than past methodologies. They have built MiniSec on Telos motes and the source code is distributed under an open-source license.

S. Kun et. al [4] have proposed a prototype of secure network access control framework in wireless sensor systems. Their configuration and implementation have effectively demonstrated the possibility of the presented technical methodologies. As their future work, they will broaden the secure access framework to help extensive wireless mesh networks.

D. Naor et. al [5] focus on the stateless receiver scenario, in which the user do not update their state from session to session. They propose a structure called the Subset-Cover framework that abstracts works a different of revocation plans including some formerly known ones. They give enough conditions that ensure the security of a revocation algorithm in this class. They illustrate two explicit Subset-Cover revocation algorithms; these algorithms are extremely adaptable and work for any number of revoked users. The plans oblige storage at the recipient of and keys separately, and keeping in mind the end goal to revoke users the obliged message lengths are of and keys individually. They give a general traitor tracing following techniques that can be coordinated with any Subset-Cover revocation plan that fulfills a "bifurcation property". This technique does not require a priori bound on the quantity of traitors and does not extend the message length by quite contrasted with the revocation of the same set of traitors. The fundamental enhancements of these techniques over existing recommended systems, when adopted to the stateless situation, are: (a) decreasing the message length to without considering the coalition size while keeping up a single decryption at the user's end (b) give a consistent integration between the revocation and tracing with the goal that the tracing techniques does not oblige any change to the revocation algorithm.

X. Lin et. al [6] have proposed a novel TSVC security plan for accomplishing proficient and secure vehicular communication, which not just meets the different security prerequisites and the driver's privacy necessity, additionally accomplish high proficiency as far as packet overhead and computation idleness are concerned. They have showed its reasonableness to real-world applications. Their present research is to explore the secure key revocation of compromised vehicles in VANETs, which is a paramount issue for any security plan.

J. Shi et. al [7] proposed a novel spatiotemporal strategy to secure range queries in event-driven two-tier sensor networks. Their method can avoid compromised master nodes from reading hosted data furthermore attains high query proficiency. Moreover, their method permits the network owner to check the legitimacy and fulfillment of any query result. Contrasted with existing work, their method can attain equivalent detection probability with very lower communication overhead in event-driven WSNs. The adequacy and productivity of their system are affirmed by detailed assessments.

L. Casado and P. Tsigas [8] proposed ContikiSec, which is a secure network layer for WSN under the Contiki operating system. They have built ContikiSec as a complete and configurable resolution, giving three security modes, beginning from privacy and integrity, and expanding to privacy, authentication and integrity. Their configuration was represented by a careful selection and careful selection investigation of previous security primitives. Their configuration attempts to attain low energy utilization without compromising security. Their assessment was carried on the MSB-430 platform, a Modular Sensor Board hardware platform made by ScatterWeb. Later on they want to study the limits of utilizing asymmetric keys as a part of their structure furthermore inspects the impact of compromised nodes in secure network layer architectures for WSNs.

D. Jinwala et. al [9] presented adaptable model of the link layer security framework for the WSNs. It is helpful in accomplishing the ideal performance in a deployed application. The resource optimization is conceivable due to the adaptability available in the hands of the application designer to choose the particular security properties as are requested really by the application. They accept that such configurable link layer security framework can simply be helpful in tuning the overhead related with diverse WSN

applications and subsequently make the whole framework more receptive to the application environment. As contrasted with the peer link layer architectures such as Tinysec, SenSec and MiniSec, they demonstrate the relative qualities of FlexiSec. Accordingly, the contribution of this examination work is in enlarging the link layer security structure for the WSNs with the new idea of configurability. They have concentrated on configurability as for the applications and the accessible resources with a fixed Mica2 hardware platform. As the applicability of the WSNs is moving out of the examination labs into these present reality areas, the exploration investigations did here need be executed for diverse stages, as well.

S. Blackshear and R. Verma [10] have presented a randomized key pre-distribution plan that opposes node compromise better than EG/HK and is not susceptible against the jamming attack that could influence Leap+ and its variations. They acquainted a method with increment the connectivity of the network while keeping the span of the key ring for every node little. Later on, they would like to built the protocol on WSN hardware and test it for vitality productivity, speed, and robustness.

3. Proposed System

MoteSec-Aware, a secure network layer protocol for WSN is presented. It meets expectations with low vitality utilization as well as creates a practical high security technique on TelosB bits, which run the TinyOS 1.X operating system. Indeed, MoteSec-Aware gives (1) a secure network protocol to allow data transmitted in an encrypted format in the air and (2) a filtering capacity to allow or deny data access based upon a set of rules, which are commonly used to ensure the information from unauthorized access while allowing authenticated communications to pass.

4. Conclusion

MoteSec-Aware is proposed and executed for TinyOS on the TelosB stage. MoteSec-Aware is a productive network layer security framework and is the completely built security technique that gives protection to both inside memory information and outside network message.

MoteSec-Aware has the capacity accomplish the objectives of substantially less energy utilization and higher security than past works. This, separated from flexibly giving a critical benefit to deployed frameworks, incredibly encourages researchers in porting their applications on lower cost and higher security platforms.

References

[1] Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, “SPINS: security protocols for sensor networks,” in Proc. 2001 International Conference on Mobile Computing and Networking.
[2] C. Karlof, N. Sastry, and D. Wagner, “TinySec: a link layer security architecture for wireless sensor networks,” in Proc. 2004 International Conference on Embedded Networked Sensor Systems.
[3] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, “MiniSec: a secure sensor network communication architecture,” in Proc. 2007 International Conference on Information Processing in Sensor Networks.
[4] S. Kun, L. An, N. Peng, and M. Douglas, “Securing network access in wireless sensor networks,” in Proc. 2009 International Conference on Wireless Network Security.
[5] D. Naor, M. Naor, and J. Lotspiech, “Revocation and tracing schemes for stateless receivers,” in Proc. CRYPTO 2001.
[6] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. (S.) Shen, “TSVC: timed efficient and secure vehicular communications with privacy preserving,” IEEE Trans. Wireless Commun., vol. 7, no. 12, Dec. 2008.
[7] J. Shi, R. Zhang, and Y. Zhang, “A spatiotemporal approach for secure range queries in tiered sensor networks,” IEEE Trans. Wireless Commun., vol. 10, no. 1, Jan. 2011.
[8] L. Casado and P. Tsigas, “Contikisec: a secure network layer for wireless sensor networks under the Contiki operating system,” in Proc. 2009 Nordic Conference on Secure IT Systems.
[9] D. Jinwala, D. Patel, and K. Dasgupta, “FlexiSec: a configurable link layer security architecture for wireless sensor networks,” Inf. Assurance and Security, vol. 4, no. 6, 2009.
[10] S. Blackshear and R. Verma, R-LEAP+: Randomizing LEAP+ Key Distribution to Resist Replay and Jamming Attacks. ACM Press, 2010.