International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey on an Efficient Data Aggregation without Data Loss with Secure Routing in Heterogeneous Wireless Sensor Networks

Shubhangi Gaikwad[1], S. V. Todkari[2]

[1]ME Computer Engineering, Jayawantrao Sawant College of Engineering, Hadapsar Pune-28,Savitribai Phule Pune University, Pune, India.

[2]Proessor and Head of Department, IT Engineering, IEEE Member, Jayawantrao Sawant College of Engineering, Hadapsar Pune28, Savitribai Phule Pune University, Pune, India.

Abstract: ***They proposed Energy expense of transmitting a solitary piece of data is around the same as that required for preparing a thousand operations in a run of the refine sensor hub. Along these lines, a reasonable approach to drag out a remote sensor system lifetime is to decrease the sensor vitality utilization in information transmissions. Information assembly is an effective approach to reduce vitality utilization on sensors. In this paper, they propose a commonsense secure information assembly plan, Sen-SDA, in view of an added substance homomorphism encryption plan, a personality based mark plan, and a bunch check system with a calculation for sifting infused false information. At that point examine the achievability of our plan utilizing ease microcontrollers picking two mainstream IEEE 802.15.4-agreeable remote sensor system equipment stages, MICAz and Tmote Sky, utilized as a part of genuine organization.***

Keywords: Wireless Sensor Networks, Data Aggregation, HE Scheme.

1. Introduction

Remote sensor systems (WSNs) are remote systems that involve a substantial number of spatially appropriated little self-directed gadgets agreeably checking natural conditions and sending the gathered information to a war room utilizing remote channels. This little gadget, called a sensor hub, comprises of handling capacity (one or more microcontrollers, CPUs or DSP chips), may contain various sorts of memory (project, information, and blaze recollections), has a RF handset (for the most part with a solitary Omni-directional receiving wire), has a force source (e.g., batteries and sun Oriented cells), and oblige different sensors and actuators. As of late, WSNs have been broadly perceived as a promising innovation that can improve different parts of today's electric force frameworks, checking portable social insurance framework and savvy transportation frameworks.

The dense and ad-hoc deployment in hazardous environment and unattended nature of WSNs make it difficult to change or recharge the node batteries. The crucial question is “how to Prolong the network lifetime to such a long time?”

Maximizing the lifetime of the network through minimizing the energy is an important challenge in WSNs. Experimental measurements have shown that generally data transmission is very expensive in terms of energy consumption (EC), while data processing consumes significantly less. Thus, a practical way to prolong the WSN lifetime is to reduce the sensor energy consumption in data transmissions.

Information collection is a productive approach to minimize vitality utilization on sensors; however it additionally makes new security challenges. A homomorphism encryption (HE) plan gives an answer for secure information total. It makes it conceivable to total n cipher texts into a solitary cipher text without utilizing any mystery keys protecting crucial math operations furthermore, classification.

2. Related Work

Kyung-Ah Shim [1] studied that, data gathering is a gainful way to deal with minimize essentialness usage on sensors, be that as it may it moreover makes new security challenges. A homomorphism encryption (HE) plan gives an answer for secure data complete. It makes it possible to all out n cipher texts into a single cipher text without using any puzzle keys securing vital math operations besides, characterization.

D. Boneh and M. Franklin [2] presented a short mark plan in view of the Computational Diffie-Hellman supposition on certain elliptic and hyper-elliptic bends. For standard security parameters, the mark length is about a large portion of that of a DSA signature with a comparative level of security. Our short mark plan is intended for frameworks where marks are written in by a human or are sent over a low-transfer speed channel. They studied various properties of our mark plan, for example, signature total and clump check.

D. Boneh [4] demonstrated that, propose a completely utilitarian personality based encryption plan (IBE). The plan has picked cipher text security in the irregular prophet model accepting a variation of the computational De- Hellman issue. Our framework depends on bilinear maps between gatherings. The Weil matching on elliptic bends is a case of such a guide. They gave exact dentitions for secure character based encryption plans and give a few applications for such frameworks.

C. Castelluccia [5] presented a remote sensor systems (WSNs) are specially appointed systems made out of modest

Licensed Under Creative Commons Attribution CC BY

gadgets with restricted calculation furthermore, vitality limits. For such gadgets, information transmission is an extremely vitality devouring operation. It hence gets to be fundamental to the lifetime of a WSN to minimize the quantity of bits sent by every gadget. One well known methodology is to total sensor information (e.g., by including) along the way from sensors to the sink. Collection turns out to be particularly testing if end-to-end) security in the middle of sensors and the sink is required. In this paper, author proposed a basic and provably secure additively homomorphism stream figure that permits efficient accumulation of encoded information. The new figure just uses particular increases (with little module) what's more, is along these lines extremely appropriate for CPU-compelled gadgets. They demonstrated that accumulation taking into account this figure can be utilized to efficiently process factual qualities for example, mean, difference and standard deviation of detected information, while accomplishing significant data transfer capacity pick up.

J. Domingo-Ferrer [6] studied, Provably Secure Additive and Multiplicative Privacy Homomorphism, Protection homeomorphisms (PHs) are encryption changes mapping an arrangement of operations on clear text to another arrangement of operations on cipher text. In the event that expansion is one of the cipher text operations, at that point it has been demonstrated that a PH is unstable against a picked clear text assault. Hence, a PH permitting full number juggling on encoded information can be best case scenario secure against known-clear text assaults. They display one such PH (none was known as such) which can be demonstrated secure against known-clear text assaults, the length of the cipher text space is much bigger than the clear text space. A few applications to assignment of touchy figuring and information and to e-betting are quickly illustrated.

J. Girao [7] proposed, Directing in remote sensor systems is not quite the same as that in rational portable specially appointed systems. It for the most part needs to bolster reverse multicast activity to one specific destination in a multichip way. For such a correspondence example, end-to-end encryption is a testing issue. To spare the general vitality assets of the system, detected information should be united and collected on its way to the last destination. They show a methodology that 1) disguises detected information end-to-end by 2) as yet giving proficient and adaptable in-system information collection. The collecting transitional hubs are not required to work on the detected plaintext information. They apply a specific class of encryption changes and examine systems for figuring the collection capacities "normal" and "development recognition." Author demonstrated that the methodology is plausible for the class of "going down" directing conventions. They consider the danger of undermined sensor hubs by proposing a key predistribution calculation that confines an aggressor's increase and appear how key redistribution and a key-ID touchy "going down" directing convention expand the power and unwavering quality of the joined spine.

V. C. Gungor observed in paper [8], that Minimizing force utilization is urgent in battery force restricted secure remote portable systems. In this paper, the author (a) present an equipment/programming set-up to measure the battery power utilization of encryption calculations through genuine living experimentation, (b) in view of the prowled information propose scientific models to catch the connections between force utilization and security, and (c) formulate and understand security augmentation subject to power imperatives. Numerical results are introduced to outline the increases that can be accomplished in utilizing arrangements of the proposed security boost issues subject to power requirements.

Sr.no	Paper Name	Technique	Advantage	Disadvantage	Result
1	Fast Batch Verification for Modular Exponentiation and Digital Signatures[3]	Focusing specifically on digital signatures, use of batching	Done very fast; in particular, They show how to screen a sequence of RSA signatures at the cost of one RSA verification plus hashing.	Recomposing is done so takes time and slows down the operation	Putting oneself above specific applications one can actually and general speed-up tools that apply to them; in particular, improve some of the mentioned works
2	Identity-Based Encryption from the Weil Pairing[4]	Bilinear map scheme is used, IBE system is used fully	can be built from any bilinear map	It takes long time for each private key generation request	Identity based encryption is to help the deployment of a public key infrastructure.
3	Efficient Aggregation of encrypted data in Wireless Sensor Networks[5]	Propose a simple and provably secure Additively homomorphism stream cipher that allows efficient aggregation of encrypted data.	Simple and secure homomorphic stream cipher that allows efficient aggregation of encrypted data	limited computation and energy capacities, communication efficiency issues	That aggregation based on this cipher can be used to efficiently compute statistical values Such as mean, variance and standard deviation of sensed data, while achieving significant bandwidth gain.
4	A Provably Secure Additive and Multiplicative Privacy Homomorphism[6]	Gambling, and more specifically electronic poker, is another recent application of the PH	Data delegation has stronger security requirements than computing delegation. In computing delegation the data handler only sees cipher text.	The equality predicate is not preserved, and thus comparisons for equality cannot be done at an unclassified level based on encrypted data	At decryption time, knowledge of the key allows the classified level to map encrypted
5	Concealed Data Aggregation for	conceals sensed data end-to-end by still providing	To save the overall energy resources of the network,	multicast traffic to one particular destination in	using this scheme for the WSN data

Licensed Under Creative Commons Attribution CC BY

	Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation[7]	efficient and flexible in-network data aggregation	sensed data needs to be consolidated and Aggregated on its way to the final destination.	a multichip manner	aggregation scenario in a higher level of security than solutions based on hop-by hop encryption

3. Architecture View

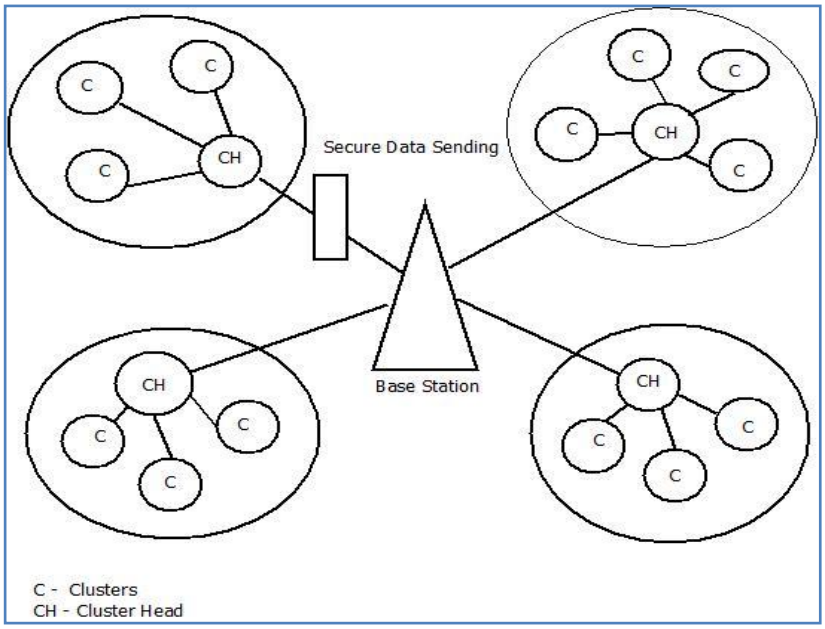

Figure 1.1: System Architecture

4. Conclusion

Cryptographic primitives are principal building squares for security conventions. It is not all that much to say that the determination furthermore, incorporation of suitable cryptographic primitives into the security plans decides the proficiency furthermore, Vitality preservation of the entire plan. In this paper, we demonstrated to incorporate an arrangement of the cryptographic primitives into a SDA plan in HSNs to accomplish security necessities. They proposed a handy SDA plan, Sen.-SDA, in light of the mix of the HE plot, ECEl Gamalþ also, the blending free IBS plan, mID-Sch and the bunch check with BQS for discovering invalid marks in heterogeneous grouped WSNs. Sen-SDA gives end-to-end secrecy and jump by-bounce validation. Autor decided the extent of a bunch depending the proportion of the quantity of invalid marks to minimize the effectiveness of CHs' bunch checks.

References

[1] Kyung-Ah Shim, Member, IEEE and Cheol-Min Park, Member, IEEE "A Secure Data Aggregation Scheme Based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 8, AUGUST 2015

[2] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in Proc. 22nd Int. Conf. Theory Appl. Cryptograph. Techn., 2003, pp. 416–432.

[3] M. Bellare, J. Garay, and T. Rabin, "Fast batch verification for modular exponentiation and digital signatures," in Proc. Adv. Cryptol. Int. Conf. Theory Appl. Cryptograph. Techn., 1998, pp. 236–250.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM J.Comput., vol. 32, no. 3, pp. 586–615, 2003.

[5] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor network, MobiQuitous '05," pp. 1–9, 2005.

[6] J. Domingo-Ferrer, "A provably secure additive and multiplicative privacy homomorphism," in Proc. 5th Int. Conf. Inf. Security, 2002, pp. 471–483.

[7] J. Girao, D. Westhoff, and M. Schneider, "CDA: Concealed data aggregation for reverse multicast traffic wireless sensor networks," in Proc. IEEE Int. Conf. Commun., 2005, pp. 3044–3049.

[8] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

Author Profile

Ms.Shubhangi Gaikwad, is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. She received her B.E (I.T) Degree from Jayawantrao Sawant College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India -411007. Her area of interest is network security, WSN.

Licensed Under Creative Commons Attribution CC BY

Prof. S. V. Todkari, received his M.E. (I.T) Degree from MIT COE KOTHRUD PUNE, Maharashtra, India. He received his B.E (CSE) Degree from college of Engineering Ambajogai, Maharashtra, India. He is currently working as H.O.D at Department of Information Technology Engineering, in Jayawantrao Sawant College of Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His area of interest is Wireless sensor network.

Licensed Under Creative Commons Attribution CC BY