IJARMATE
Your ulti-MATE Research Paper !!!

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 8, August 2016.

Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence Of Collusion Attacks

Ragavi T, M.Phil,
Department of Computer Science,
Mother Teresa University,
Chennai- 15

Dr.S.Lakshmi
Assistant Professor
Department of Computer Science and Engineering,
Jeppiaar Engineering College ,
Chennai-600 004

Abstract:

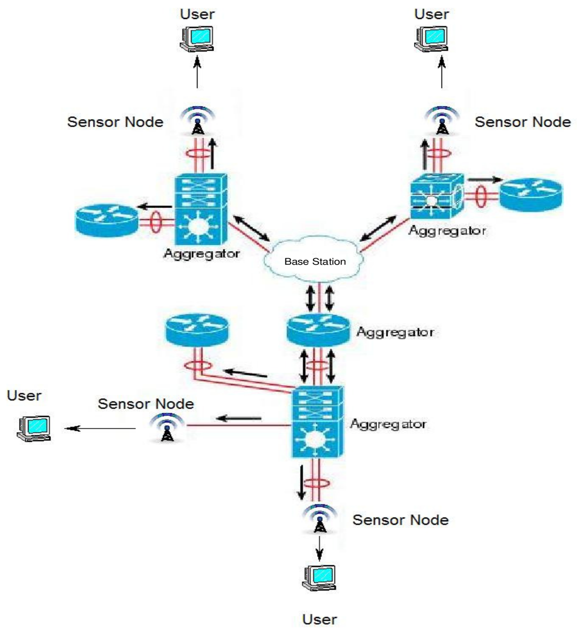
Wireless sensor networks generally abide of a ample bulk of bargain sensor nodes that accept carefully bound sensing, computation, and advice capabilities. Due to ability belted sensor nodes, it is important to abbreviate the bulk of abstracts manual so that the boilerplate sensor lifetime and the all-embracing bandwidth appliance are improved. Abstracts accession is the action of summarizing and accumulation sensor abstracts in adjustment to abate the bulk of abstracts manual in the network. This cardboard investigates the accord amid aegis and abstracts accession action in wireless sensor networks. We authenticate that several absolute accepted clarification algorithms while decidedly added able-bodied adjoin bunco attacks than the simple averaging methods, are about affect able to a atypical adult bunco advance we introduce. To abode this aegis issue, we adduce an advance for accepted clarification techniques by accouterment an antecedent approximation for such algorithms which makes them not alone bunco robust, but as well added authentic and faster converging.

Key Word: Wireless sensor, encryption, decryption

1. INTRODUCTION

Due to a charge for robustness of ecology and low amount of the nodes, wireless sensor networks (WSNs) are usually redundant. Abstracts from assorted sensors is aggregated at an aggregator bulge which again assiduously to the abject base alone the accumulated values. At present, due to limitations of the accretion ability and activity ability of sensor nodes, abstracts are aggregated by acutely simple algorithms such as averaging. However, such accession is accepted to be actual accessible to faults, and added importantly, awful attacks [1]. This cannot be remedied by cryptographic methods, because the attackers about accretion complete admission to advice stored in the compromised nodes. For that acumen abstracts accession at the aggregator bulge has to be accompanied by an appraisal of abidingness of abstracts from alone sensor nodes. Thus, better, added adult algorithms are bare for abstracts accession in the approaching WSN. Such an algorithm should accept two features. 1. In the attendance of academic errors such algorithm should aftermath estimates which are abutting to the optimal ones in advice academic sense. Thus, for example, if the babble present in anniversary sensor is a Gaussian apart broadcast babble with aught mean, again the appraisal produced by such an algorithm should accept a about-face abutting to the Cramer-Rao lower apprenticed (CRLB) [2], i.e, it should be abutting to the about-face of the Maximum Likelihood Estimator (MLE). However, such admiration should be accomplished after bartering to the algorithm the variances of the sensors, bare in practice. 2. The algorithm should as well be able-bodied in the attendance of non-stochastic errors, such as faults and awful attacks, and, besides accumulation data, such algorithm should as well accommodate an appraisal of the believability and abidingness of the abstracts accustomed from anniversary sensor node.

2. METHODOLOGY:



System architecture diagram

Secure encrypted-data aggregation for wireless sensor networks

This paper proposes a secure encrypted-data aggregation scheme for wireless sensor networks. Our design for data aggregation eliminates redundant sensor readings without using encryption and maintains data secrecy and privacy during transmission. Conventional aggregation functions operate when readings are received in plaintext. If readings are encrypted, aggregation requires decryption creating extra overhead and key management issues. In contrast to conventional schemes, our proposed scheme provides security and privacy, and duplicate instances of original readings will be aggregated into a single packet. Our scheme is resilient to known-plaintext attacks, chosen-plaintext attacks, cipher text-only attacks and man-in-the-middle attacks. Our experiments show that our proposed aggregation method significantly reduces communication overhead and can be practically implemented in on-the-shelf sensor platforms.

3. LITREATURE REVIEW:

In A Rate-Adaptive MAC Protocol for Multi-Hop Wireless Networks, Gavin Holland and NitinVaidya proposed that the topic of optimizing performance in wireless local area networks using rate adaptation. We presented a new approach to rate adaptation, which differs from previous approaches in that it uses the RTS/CTS protocol to enable receiver-based rate adaptation. Usingthis approach, a protocol based on the popular IEEE 802.11 standard was presented, called the Receiver-Based AutoRate (RBAR) protocol.

In Modulation Rate Adaptation in Urban and Vehicular Environments: Cross-layer Implementation andExperimental

Evaluation, Joseph Camp and Edward Knightly proposed a custom cross-layer rate adaptation framework which has high levels of interaction and observability between MAC and PHY layers. We are the first to implement SNR-based rate adaptation at MAC time scales comparable to commercial systems and evaluate protocol accuracy compared to optimal rate selection on a packet-by-packet basis.. Finally, we show that a mechanism designed to equally share throughput in the hidden terminal scenario has a severe imbalance in throughput sharing with only slight heterogeneity in average link quality of competing transmitters

In Efficient Channel-aware Rate Adaptation in Dynamic Environments, Glenn Judd andXiaohui Wang proposed that their results in highly dynamic wireless channels, which can affect the performance of many aspects of the mobile device. Adaptation is critical to overall system performance. We use time-aware signal prediction technique to predict current channel information based on past observations, thus avoiding the pitfall of using stale channel information. In addition, we have developed techniques for automatically calibrating SINR thresholds.

In Cross-Layer Wireless Bit Rate Adaptation, MythiliVutukuru and HariBalakrishnan proposed chieves throughput gains of up to 2 over frame-based protocols such as SampleRate and RRAA, 20% over SNR-based protocols trained on the operating environment, and 4 over untrained SNR-based protocols. The key idea is to expose per-bit confidences called SoftPHY hints from the physical layer, using them to estimate the interference-free BER of received frames. Picking bit rates using the BER thus estimated enables SoftRate to react quickly to channel variation without requiring any environment-specific calibration. Moreover, SoftRate's idea of estimating BER from SoftPHY hints can be applied to a variety of wireless cross-layer protocols that, for example, allocate frequency or transmit power, or perform efficient error recovery.

In Cross-Layer Architecture for Adaptive Video Multicast Streaming OverMultirate Wireless LANs, Pedro Cuenca and Luis Orozco-Barbosa proposed a cross-layer architecture for adaptive video multicast streaming over multirate wireless LANs where layer-specific information is passed in both directions, top-own and bottom-up. This architecture requires knowing the operating conditions of the channel as perceived by the multicast members. The PHY data rate to be used for the multicast traffic is determined based on the feedback received by the group leader. We have also paid particular attention to limit the overhead introduced by the multicast rate adaptation mechanism. We have considered jointly three layers of the protocol stack: the application, data link and physical layers.

4. CONCLUSION AND FUTURE WORK:

In this paper, we introduced a novel collusion attack scenario against a number of existing IF algorithms. Moreover, we proposed an improvement for the IF algorithms by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms not only collusion robust, but also more accurate and faster converging.

In future work, we will investigate whether our approach can protect against compromised aggregators. We also plan to implement our approach in a deployed sensor network.

5. REFERENCES

[1] S. Ozdemir and Y. Xiao, “Secure data aggregation in wireless sensor networks: A comprehensive overview,” Comput. Netw., vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[2] L. Wasserman, All of Statistics : A Concise Course in Statistical Inference. New York, NY, USA: Springer,.

[3] A. Jøsang and J. Golbeck, “Challenges for robust trust and reputation systems,” in Proc. 5th Int. Workshop Security Trust Manage., Saint Malo, France, 2009, pp. 253–262.

[4] K. Hoffman, D. Zage, and C. Nita-Rotaru, “A survey of attack and defense techniques for reputation systems,” ACM Comput. Surveys, vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.

[5] R. Roman, C. Fernandez-Gago, J. Lopez, and H. H. Chen, “Trust and reputation systems for wireless sensor networks,” in Security and Privacy in Mobile and Wireless Networking, S. Gritzalis, T. Karygiannis, and C. Skianis, eds.,Leicester, U.K.: Troubador Publishing Ltd, 2009 pp. 105–128,.

[6] H.-S. Lim, Y.-S. Moon, and E. Bertino, “Provenance-based trustworthiness assessment in sensor networks,” in Proc. 7th

Int. Workshop Data Manage. Sensor Netw., 2010, pp. 2–7.

[7] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN," in Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput., 2011, pp. 1–4.

[8] C. de Kerchove and P. Van Dooren, "Iterative filtering in reputation systems," SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.

[9] Y. Zhou, T. Lei, and T. Zhou, "A robust ranking algorithm to spamming," Europhys. Lett., vol. 94, p. 48002, 2011.

[10] P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, "Information filtering via iterative refinement," Europhys. Lett., vol. 75, pp. 1006– 1012, Sep. 2006.

[11] Y.-K. Yu, Y.-C. Zhang, P. Laureti, and L. Moret, "Decoding information from noisy, redundant, and intentionally distorted sources," Physica A: Statist. Mech. Appl., vol. 371, pp. 732–744, Nov. 2006.

[12] R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, "Robust reputationbased ranking on bipartite rating networks," in Proc. SIAM Int. Conf. Data Mining, 2012, pp. 612–623.

[13] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," Proc. IEEE Int. Conf. Symp. Inf. Theory, vol. 3, 2009, pp. 2051–2055.

[14] H. Liao, G. Cimini, and M. Medo, "Measuring quality, reputation and trust in online communities," in Proc. 20th Int. Conf. Found. Intell. Syst., Aug. 2012, pp. 405–414.

[15] B.-C. Chen, J. Guo, B. Tseng, and J. Yang, "User reputation in a comment rating environment," in Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2011, pp. 159–167.

[16] C. T. Chou, A. Ignatovic, and W. Hu, "Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 8, pp. 1525–1534, Aug. 2013.

[17] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," J. Netw. Comput. Appl., vol. 35, no. 3, pp. 867–880, 2012.