ISSN: 2321-7782 (Online)
Volume 2, Issue 2, February 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Homomorphic Encryption Based Privacy Preservation against Traffic Analysis in Wireless Networks

Sumathi Sivaraj[1]
M. E Computer Science and Engineering
Sri Eshwar College of Engineering
Coimbatore – India

L. Dhanam[2]
M. E Computer Science and Engineering
Sri Eshwar College of Engineering
Coimbatore – India

S. Mohana Gowri[3]
M. E Computer Science and Engineering
Sri Eshwar College of Engineering
Coimbatore – India

P. Dhivya[4]
M. E Computer Science and Engineering
Sri Eshwar College of Engineering
Coimbatore – India

R. Vanathi[5]
M. E Computer Science and Engineering
Sri Eshwar College of Engineering
Coimbatore – India

Abstract: ***Privacy threat is one in every of the essential problems in multi-hop wireless networks, wherever attacks like traffic analysis and flow tracing will be simply launched by a malicious opponent because of the open wireless medium. Network cryptography has the potential to thwart these attacks since the coding/mixing operation is inspired at intermediate nodes. However, the straightforward readying of network cryptography cannot come through the goal once enough packets area unit collected by the adversaries. On the opposite hand, the coding/mixing nature precludes the practicableness of using the prevailing privacy-preserving techniques, like Onion Routing. During this paper, we have a tendency to propose a completely unique network cryptography based mostly privacy-preserving theme against traffic analysis in multi-hop wireless networks. With homomorphic cryptography, the projected theme offers 2 vital privacy-preserving options, packet flow untraceability and message content confidentiality, for expeditiously thwarting the traffic analysis attacks. Moreover, the projected theme keeps the random cryptography feature. Theoretical analysis and simulative analysis demonstrate the validity and potency of the projected theme.***

Keywords: Homographic encryption, sensor node, network coding, traffic analysis.

I. INTRODUCTION

Multi_hop Wireless Networks are considered such a promising answer for extending the radio coverage varies of the present wireless networks. There exist several security and privacy problems in MWN. Due to the open try wirless transmission, MWN's suffer from varied types of attacks, such as eaves dropping, data modification and node compromising these attacks could breach the protection properties of MWNs, including confidentiality, integrity, and genuineness. Reputation-based mechanisms and incentive protocols have been projected to guard against packet visit enforcing and stimulating the nodes' cooperation, respectively. For reputation-based mechanisms, every node has monitors the transmissions of its neighbours to form sure that the neighbours relay others' traffics and therefore the uncooperative nodes (malicious or selfish) will be identified and tarred-and-feathered. Every node maintains a name value for every neighbour. A neighbour's name price is improved once the neighbour relays a packet and degraded when the neighbour drops a packet.

In this paper we tend to specialize in privacy preservation problems that are how to stop traffic analysis/flow tracing and achieve source namelessness in MWN's. Source namelessness is special interest in MWN's, Source namelessness refers to communicating through a network while not revealing the identity or location of the supply node. Preventing traffic analysis/flow tracing and provising supply namelessness is critical for securing MWNs. Where the nodes will communicate with one another through multi_hop packet forwarding. Existing privacy preservation answer, like proxy _based schemes, Chum's combine _based theme, e.g. with an end_to_end delay of many minutes. During this paper based mostly on network cryptography and homomorphy encoding functions. We propose AN economical privacy_prserving theme for MWNs. Our objective is to realize supply namelessness by preventing traffic analysis and flow tracing attacks.

The projected theme offers the subsequent enticing features

A. Increased Privacy against flow tracing and traffic analysis the confidentiality of GEVs is effectively secure, which makes it tough for attackers to recover the GEVs.

B. Efficiency Due to the homomorphy of HEFs, messages recoding at intermediate nodes will be directly performed on encrypted GEVs and encoded massages, without knowing the cryptography key or acting the decryption operation on every incoming packet.

C. High invertible GEVs Random network cryptography is possible as long as the Prefixed GEVs are Inverible.

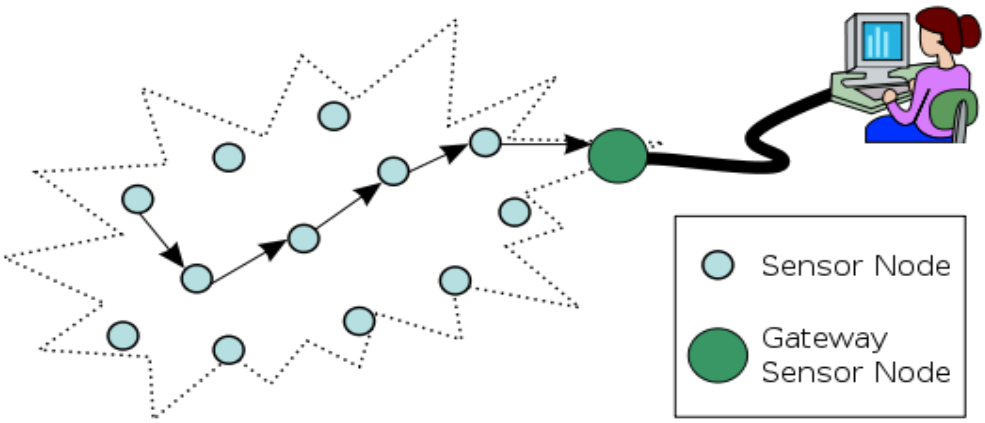

Figure 1.1 Wireless Sensor Architecture

II. OBJECTIVE

1. Input style is that the method of changing a user-oriented description of the input into a computer-based system. This style is very important to avoid errors within the knowledge input method and show the right direction to the management for obtaining correct data from the processed system.

2. It's achieved by making easy screens for the information entry to handle giant volume of knowledge. The goal of coming up with input is to create knowledge entry easier and to be free from errors. The information entry screen is intended in such how that each one the information manipulates may be performed. It additionally provides record viewing facilities.

3. When the information is entered it'll check for its validity. Knowledge may be entered with the assistance of screens. Applicable messages area unit provided as once required so the user won't be in maize of instant. Therefore the target of input style is to form AN input layout that's simple to follow.

III. PROPOSED SYSTEM

This concept describes, we tend to concentrate on the privacy issue, i.e., the way to stop traffic analysis/flow tracing and bring home the bacon supply obscurity in MWNs. Another example is that the event reportage in wireless detector networks,

wherever flow tracing will facilitate attackers to spot the placement of involved events, e.g., the looks of AN vulnerable animal during a monitored space, so take sequent actions to capture or kill the animals. Among all privacy properties, supply obscurity is of interest group in MWNs. supply obscurity refers to human action through a network while not revealing the identity or location of supply nodes. Additionally, some advanced attacks, like traffic analysis and flow tracing, can even be launched by a malicious someone to compromise users' privacy, as well as supply obscurity and traffic secrecy.

1. Attackers Modules:

The appearance of associate vulnerable animal (Attackers) in a very monitored space is survived by wireless device, at the on every occasion the inside and outdoors sensors square measure sensing to search out out the attackers location and also the temporal arrangement. This data is passed to the server for analyzing. Once analyzing the commander and Hunter they're can also participate this wireless network. within the commander and hunter itself some intruders square measure there, our aim is to capture the attackers before making an attempt the network.

2. Homomorphic Encoding Functions:

The homomorphic encoding operate is extremely potency and securable. within the Commander method, we have a tendency to exploitation this for every packet encoding .Due to the similarity of HEFs, message cryptography at intermediate nodes may be directly performed on encrypted and encoded messages, while not knowing the secret writing keys or performing arts high-priced secret writing operations on every incoming packet. The performance analysis on procedure quality demonstrates the potency of the projected theme. Homomorphic encoding Functions (HEFs) have the property of similarity, which implies operations on plaintext may be performed by operational on corresponding cipher text.

3. Threat models:

Outside Attacker: An out of doors aggressor is thought of as a worldwide passive auditor United Nations agency has the flexibility to watch all network links, as shown in Fig. an out of doors aggressor will examine the tags and message content, and so link outgoing packets with incoming packets. Further, even though end-to-end encoding is applied to messages at a better layer, it's still potential for a worldwide outside aggressor to trace packets by analyzing and scrutiny the message cipher text.

Inside Attacker: An internal attacker might compromise many intermediate nodes, as shown in Fig. Link-to -link encoding is at risk of within attackers since they'll have already got obtained the decipherment keys and so the message plaintext is simply recovered. Each among and outdoors attackers may perform extra advanced traffic analysis/flow tracing techniques, still as size correlation, time correlation, and information content correlation.

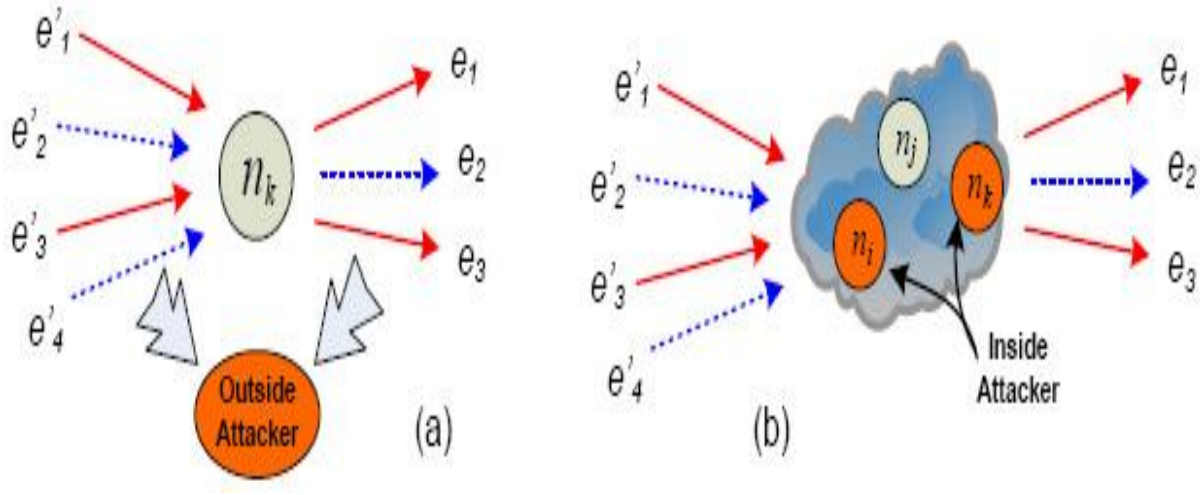

Figure 3.1 Enhanced Privacy against traffic analysis and flow tracing:

With the utilization of HEFs, the confidentiality of GEVs is effectively bonded, creating it troublesome for attackers to recover the plaintext, not like alternative packet-forwarding systems, network secret writing permits intermediate nodes to perform computation on incoming messages, creating outgoing messages be the mixture of incoming ones. Flow tracing within the sense of the report concerning the alerting sensing element.

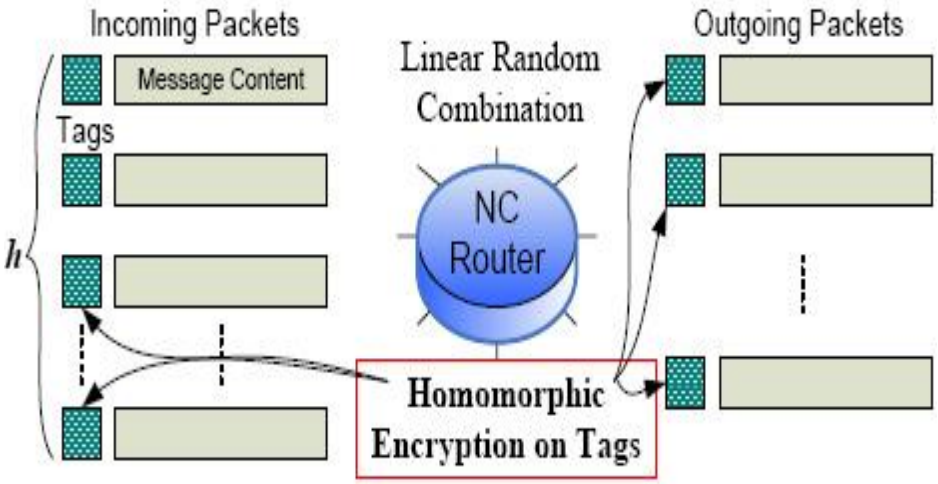

Figure 3.2 Homomorphic Encryption on Tags

4. Security Analysis:

The generation variety of a packet is hidden within the secure routing theme through link-to-link cryptography. During this means, attackers cannot realize the generation variety of a packet for his or her more analysis. Notice that secure routing methods are solely needed to be established at the start of every session; throughout the packet transmission, secure routing methods aren't needed to vary or re-established for every new generation.

IV. CONCLUSION

This Project explains, we've got planned associate economical network cryptography primarily based privacy-preserving theme against traffic analysis and flow tracing in multi-hop wireless networks. With the light-weight homomorphic coding on world coding Vectors (GEVs), the planned theme offers 2 vital privacy conserving options, packet flow untraceability and message content confidentiality; this could expeditiously thwart traffic analysis/flow tracing attacks. Moreover, with homomorphic coding, the planned theme keeps the essence of random linear network cryptography, and every sink will recover the supply messages by inverting the GEVs with a really high likelihood. The mensuration and simulative analysis on privacy Enhancement and procedure overhead demonstrate the effectiveness and potency of the planned theme.

References

1. User Interfaces in C#: Windows Forms and Custom Controls by Matthew MacDonald.
2. Applied Microsoft® .NET Framework Programming (Pro-Developer) by Jeffrey Richter.
3. Practical .Net2 and C#2: Harness the Platform, the Language, and the Framework by Patrick Smacchia.
4. Data Communications and Networking, by Behrouz A Forouzan.
5. Computer Networking: A Top-Down Approach, by James F. Kurose.
6. Operating System Concepts, by Abraham Silberschatz.Amichai-Hamburger, Y., Fine, A., & Goldstein, A. (2004). The impact of Internet interactivity and need for closure on consumer preference. Computers in Human Behavior, 20, 103-117.
7. Balabanis, G., Reynolds, N., & Simintiras, A. (2006). Bases of e-store loyalty: Perceived switching barriers and satisfaction. Journal of Business Research, 59, 214-224.
8. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *the Proceedings of IEEE Conference on Privacy and Security*,1996, pp. 164–173.
9. M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis, "The keynote trust-management system, version 2," in *RFC 2704*,
10. G. Karjoth, "The authorization service of tivoli policy director," in *the Proceedings of the 17th Computer Security Applications Conference (ACSAC)*, December 2001, p. 319.

11. S. Ioannidis, A. Keromytis, S. Bellovin, and J. Smith, Implementing a distributed firewall," in *the Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2000, pp. 190–199.
12. W. R. Cheswick, S. M. Bellovin, and A. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker*, 2nd ed. Addison-Wesley, 2003.
13. M. Christiansen and E. Fleury, "Using interval decision diagrams for packet filtering," 2002, http://www.cs.auc.dk/ fleury/publications.html.
14. E. Cohen and C. Lund, "Packet classification in large ISPs: Design and evaluation of decision tree classifiers," in *Proc. ACM SIGMETRICS*. New York, NY, USA: ACM Press, 2005, pp. 73–84.
15. S. Crosby and D. Wallach, "Denial of service via algorithmic complexity attacks," in *Proceedings of the 12th USENIX Security Symposium*, August 2003, pp. 29–44.
16. M. de Berg, M. van Kreveld, and M. Overmars, *Computational Geometry: Algorithms and Applications*, 2nd ed. Springer-Verlag, 2000.

AUTHOR(S) PROFILE

S. SUMATHI received her MCA Degree from Bharathiyar University Coimbatore, Tamilnadu, India and pursuing M.E (Computer Science and Engineering) degree from Sri Eshwar College of Engineering Coimbatore, India. Her area of interest is Network security and Cloud Computing.

L. DHANAM received her B.E(CSE) Degree from Hindusthan college of Engineering and Technology, Coimbatore, Tamilnadu, India and pursuing M.E (CSE) Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her field of Interest is Network security, Operating system and Theory of Computation.

S.MOHANA GOWRI received her B.Tech(IT) Degree from Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamilnadu, India and pursuing M.E Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her fields of Interest are Network Security, Operating systems and Software Engineering.

P.DHIVYA received her B.Tech(IT) Degree from P.A College of Engineering, Pollachi, Tamilnadu, India and pursuing M.E Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her fields of Interest are Network Security, Operating systems and Data structures.

R.VANATHI received her B.E (CSE) Degree from Info Institute of Engineering, Coimbatore, Tamil Nadu, India and pursuing M.E (CSE) Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her fields of Interest are Cryptography and Network security, Database Management System and Operating System.

