International Organization of Research & Development (IORD)
ISSN: 2348-0831
Vol 01 Issue 01 | 2013

ENHANCE APPROACH FOR MESSAGE AUTHENTICATION AND SOURCE PRIVACY PRESERVING IN WIRELESS NETWORK

Nilesh R. Belkhede[1], Yogesh Bhute[2]
Department Of Computer Science and Engineering, Abha Gaikwad Patil College Of Engineering Nagpur,India.
nlshbelkhede67@gmail.com, yog.bhute@gmail.com

Abstract:
Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless networks. For this reason, many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. To address these issues, a polynomial-based scheme was recently introduced. However, this scheme and its extensions all have the weakness of a built-in threshold determined by the degree of the polynomial when the number of messages transmitted is larger than this threshold, the adversary can fully recover the polynomial.
Keyword: Message authentication, symmetric-key cryptosystem, public-key cryptosystem, source privacy, wireless network.

I. INTRODUCTION

Message authentication plays a key role in thwarting unauthorizedand corrupted messages from being forwarded innetworks to save the precious sensor energy. For this reason,many authentication schemes have been proposed in literatureto provide message authenticity and integrity verification forwireless sensor networks (WSNs) [1]–[5]. These schemes canlargely be divided into two categories: public-key based approachesand symmetric- key based approaches.The symmetric-key based approach requires complex keymanagement, lacks of scalability, and is not resilient to largenumbers of node compromise attacks since the message senderand the receiver have to share a secret key. The shared keyis used by the sender to generate a message authenticationcode (MAC) for each transmitted message. However, for thismethod, the authenticity and integrity of the message can onlybe verified by the node with the shared secret key, which isgenerally shared by a group of sensor nodes. An intruder cancompromise the key by capturing a single sensor node. Inaddition, this method does not work in multicast networks.

To solve the scalability problem, a secret polynomial basedmessage authentication scheme was introduced in [3]. The ideaof this scheme is similar to a threshold secret sharing, where thethreshold is determined by the degree of the polynomial. Thisapproach offers information-theoretic security of the sharedsecret key when the number of messages transmitted is less thanthe threshold. The intermediate nodes verify the authenticityof the message through a polynomial evaluation. However,when the number of messages transmitted is larger than thethreshold, the polynomial can be fully recovered and the systemis completely broken.Key distribution is acentral problem in cryptographic systems, and is a majorcomponent of the security subsystem of distributed systems, communicationsystems, and data networks. The increase in bandwidth, size, usage, and applicationsof such systems is likely to pose new challenges and to require novel ideas. A growing application area in networking is “conferencing” a group ofentities (or network locations) collaborate privately in an interactive procedure(such **as:** board meeting, scientific discussion, a task-force, a classroom, or abulletin- board). In this work we consider perfectly-secure key distribution forconferences. (Note that key distribution for two-party communication (session key)is a special case of Conferences of size two).If users of a group (a conference) wish to communicate in a network usingsymmetric encryption, they must share a common key. A key distributionscheme (denoted KDS for short) is a method to distribute initial private piecesof information among a set of users, such that each group of a given size (or upto a given size) can compute a common key for secure conference. This informationis generated and distributed by a trusted server which is active only at thedistribution phase.

II. LITERATURE SURVEY

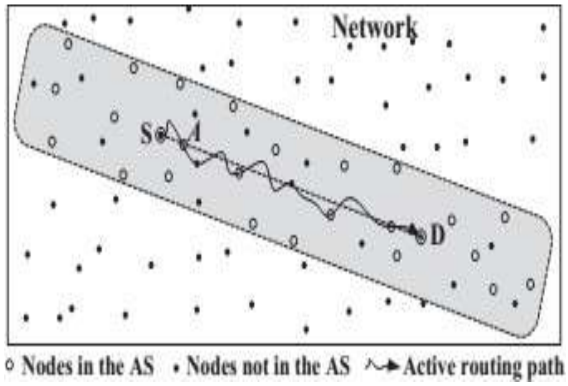

Fig. block diagram of existing system

In the fig S is the source node and D is the destination node. In the existing system data directly transfer to the end user. Source node request for the acknowledgement for the transmission and D give the acknowledgement then transmission is done only. Before a message is transmitted, the message source node selects an AS from the public key list in the SS as its choice. This set should include itself, together with some other nodes. When an adversary receives a message, he can possibly find the direction of the previous hop, or even the real node of the previous hop. However, the adversary is unable to distinguish whether the previous node is the actual source node or simply a forwarder node if the adversary is unable to monitor the traffic of the previous hop. Therefore, the selection of the AS should create sufficient diversity so that it is infeasible for theAdversary to find the message source based on the selection of the AS itself.

Jian Li *et al.* [1] "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks" in this paper author propose a scalable authentication scheme based onelliptic curve cryptography (ECC). While enabling intermediatenodes authentication, our proposed scheme allows any node totransmit an unlimited number of messages without suffering thethreshold problem. In addition, our scheme can also providemessage source privacy. Both theoretical analysis and simulationresults demonstrate that our proposed scheme is more efficientthan the polynomial-based approach in terms of computationaland communication overhead under comparablesecurity levelswhile providing message source privacy.

Technique use:

Proposed source anonymous messageauthentication (sama) on elliptic curves Author says propose an unconditionally secure andefficient source anonymous message authentication scheme (SAMA). The main idea is that for each message *m* to bereleased, the message sender, or the sending node, generatesa source anonymous message authenticator for the message*m*. The generation is based on the MES scheme on ellipticcurves. For a ring signature, each ring member is required tocompute a forgery signature for all other members in the AS.In our scheme, the entire SAMA generation requires only threesteps, which link all non-senders and the message sender to theSAMA alike. In addition, our design enables the SAMA to beverified through a single equation without individually verifyingthe signatures. [1]

Carlo Blundolz*et al.* [2] "Perfectly-Secure Key Distribution for DynamicConferences" Author in this paper proposed a key distribution scheme for dynamic conferences is a methodby which initially an (off-line) trusted server distributes private individualpieces of information to a set of users. Later any group of users of agiven size (a dynamic conference) is able to compute a common securekey. In this paper we study the theory and applications of such perfectlysecure systems, in this setting, any group of t users can computea common key by each user computing using only his private piece ofinformation and the *identities* of the other *t* - 1 group users. Keys aresecure against coalitions of up to *k* users, that is, even if *E* users pooltogether their pieces they cannot compute anything about a key of anyt-size conference comprised of other users. A key distribution scheme for dynamic conferences is a methodby which initially an (off-line) trusted server distributes private individualpieces of information to a set of users. Later any group of users of agiven size (a dynamic conference) is able to compute a common securekey. In this paper we study the theory and applications of such perfectlysecure systems, in this setting, any group of t users can computea common key by each user computing using only his private piece ofinformation and the *identities* of the other *t* - 1 group users. Keys aresecure against coalitions of up to *k* users, that is, even if *E* users pooltogether their pieces they cannot compute anything about a key of anyt-size conference comprised of other users. Technique use A key distributionscheme (indicated by KDS for short) distributes some information amonga set of users, so that any *t* of them can join and generate a secure key, weassumea trusted off-line server active only at initiation (unlike an on-line serverapproach put forth in [I91 which we call server-based KDS). We say the systemis k-secure if any *k* users, pooling together their pieces, have no information onkeys they should not know. These schemes can be further classified into two categories:interactive (where users are engaged in a protocol, prior to usage of thecommon key), and non-interactive where keys are generated privately by the individuals.Next, we formally define non-interactive key distribution schemes. Ourdefinition of security is based on the notion of entropy and is thus unconditional. [2]

Fan Ye, *et al.* [3] “Statistical En-route Filtering of Injected False Datain Sensor Networks” in this paper author propose In a large-scale sensor network individual sensorsare subject to security compromises. A compromised node caninject into the network large quantities of bogus sensing reportswhich, if undetected, would be forwarded to the data collectionpoint (i.e. the sink). Such attacks by compromised sensors cancause not only false alarms but also the depletion of the finiteamount of energy in a battery powered network. In this paper wepresent a Statistical En-route Filtering (SEF) mechanism that candetect and drop such false reports. SEF requires that each sensingreport be validated by multiple keyed message authenticationcodes (MACs), each generated by a node that detects the sameevent. As the report is forwarded, each node along the wayverifies the correctness of the MACs probabilistically and dropsthose with invalid MACs at earliest points.Technique use Statistical En-route Filteringmechanism (SEF). SEF exploits the sheer scale and densedeployment of large sensor networks. To prevent any singlecompromised node from breaking down the entire system, SEFcarefully limits the amount of security information assignedto any single node, and relies on the collective decisions ofmultiple sensors for false report detection. When a sensingtarget (henceforth called “stimulus” or “event”) occurs inthe field, multiple surrounding sensors collectively generate alegitimate report that carries multiple message authenticationcodes (MACs) Statistical En-route Filteringmechanism (SEF). SEF exploits the sheer scale and densedeployment of large sensor networks. To prevent any singlecompromised node from breaking down the entire system, SEFcarefully limits the amount of security information assignedto any single node, and relies on the collective decisions ofmultiple sensors for false report detection. When a sensingtarget (henceforth called “stimulus” or “event”) occurs inthe field, multiple surrounding sensors collectively generate alegitimate report that carries multiple message authenticationcodes (MACs) [3].

Wensheng Zhang*et al.* [4] “Lightweight and Compromise-Resilient MessageAuthentication in Sensor Networks” author deals with numerous authentication schemes have been proposed in the past for protecting communication authenticity andintegrity in wireless sensor networks. Most of them howeverhave following limitations: high computation or communicationoverhead, no resilience to a large number of node compromises,delayed authentication, lack of scalability, etc. To address theseissues, we propose in this paper a novel message authenticationapproach which adopts a perturbed polynomial-based technique to simultaneously accomplish the goals of lightweight, resilience toa large number of node compromises, immediate authentication,scalability, and non-repudiation. Extensive analysis and experiments have also been conducted to evaluate the scheme in termsof security properties and system overheadsensor network that consists of a base stationand a certain number of sensor nodes, where each sensor nodecan be a data source or a data sink. The network supportthe following communication patterns: (i) the base stationbroadcasts/multicasts messages to all or a certain set of sensornodes; (ii) a sensor node broadcasts/multicasts messages to allor a certain set of other sensor nodes; (iii) the base stationuncast messages to a certain sensor node; and (iv) a sensornode uncast messages to the base station or a certain sensornode. The above communication patterns may be either synchronous (i.e., the receivers are available to receive messages when messages are disseminated) or asynchronous (i.e., whena sender disseminates messages, some desired receivers maynot be available; after becoming available, the receivers may obtain the messages from other receivers that have received and cached the messages.

Adrian Perrig*et al.* [5] “Efficient Authentication and Signing ofMulticast Streams over Lossy Channels” Multicast stream authentication and signing is an important and challenging problem. Applications include thecontinuous authentication of radio and TV Internet broadcasts, and authenticated data distribution by satellite. Themain challenges are fourfold. First, authenticity must beguaranteed even when only the sender of the data is trusted.

Second, the scheme needs to scale to potentially millions ofreceivers. Third, streamed media distribution can have highpacket loss. Finally, the system needs to be efficient to support fast packet rates.We propose two efficient schemes, TESLA and EMSS,for secure lossy multicast streams. TESLA, short for TimedEfficient Stream Loss-tolerant Authentication, offers senderauthentication, strong loss robustness, high scalability, andminimal overhead, at the cost of loose initial time synchronization and slightly delayed authentication. EMSS, shortfor Efficient Multi-chained Stream Signature, provides nonrepudiation of origin, high loss resistance, and low overhead, at the cost of slightly delayed verification technique use TESLA: Timed Efficient Stream Losstolerant AuthenticationIn this section, we describe five schemes for stream authentication. Each scheme builds up on the previous oneand improves it to solve its shortcomings. Finally, schemeV, which we call TESLA (short for Timed Efficient StreamLoss- tolerant Authentication), satisfies all the properties welisted in the introduction. The cryptographic primitives usedin this section are reviewed in Appendix A, which also contains a sketch of a security analysis for our scheme.We use the following notation:hx; yidenotes the concatenation ofxandy,Sstands for sender, andRstands forreceiver.

III. CONCLUSION

By applying proposed algorithm we will get Message Authentication and source Privacy Preserving in Wireless Network. We preserving the privacy of the user and provide a strong and energy efficient algorithm for the data encryption.

A propose method will efficient that other existing system because there is no privacy preservation in existing system. And for transmission we will encrypt by using RC6 algorithm. It’s very efficient than existing algorithm.

REFERENCES

[1] Jian Li Yun Li JianRenJie Wu *“Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks”* 1045-9219/13/$31.00 © 2013 IEEE

[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, *“An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks,”* in *IEEE Symposium on Security and Privacy*, 2004.

[3] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, *“Perfectly- secure key distribution for dynamic conferences,” in Advances in Cryptology - Crypto’92,* ser. Lecture Notes in ComputerScience Volume 740, 1992, pp. 471–486.

[4] W. Zhang, N. Subramanian, and G. Wang, *“Lightweight and compromiseresilient message authentication in sensor networks,”* in *IEEE INFOCOM*, Phoenix, AZ., April 15-17 2008.

[5] A. Perrig, R. Canetti, J. Tygar, and D. Song, *“Efficient authentication and signing of multicast streams over lossy channels,”* in *IEEE Symposium on Security and Privacy*, May 2000.

[6] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, *“Attacking cryptographic schemes based on “perturbation polynomials”,* Cryptology ePrint Archive, Report 2009/098, 2009, http://eprint.iacr.org/.

[7] R. Rivest, A. Shamir, and L. Adleman, *“A method for obtaining digital signatures and public-key cryptosystems,” Communications. of the Assoc. of Comp. Mach.*, vol. 21, no. 2, pp. 120–126, 1978.

[8] T. A. ElGamal, “*A public-key cryptosystem and a signature scheme based on discrete logarithms,”IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[9] H. Wang, S. Sheng, C. Tan, and Q. Li, *“Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control,” in IEEE ICDCS,* Beijing, China, 2008, pp. 11–18.