The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 3 || Pages || PP.33-38|| 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Message Authentication And Source Privacy Using BAC Technique In Wireless Sensor Networks

[1,] G.Dhivya, [2,] N.R.Jayashree MCA.,M.Tech
[1,] PG Student, [2,] Assistant Professor
[1,]dhivyagunasekaran2@gmail.com,[2,]meeesai77@yahoo.in
Jayam College Of Engineering and Technology Dharmapuri(DT), Tamilnadu.

ABSTRACT

A scalable authentication scheme is based on elliptic curve Cryptography (ECC), while enabling intermediate nodes authentication, our existing scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, existing scheme can also provide message source privacy and did not provide destination privacy. In this propose work a novel method, Data-Transparent Authentication (DaTA) without Communication Overhead, to validate data streams. Our strategy neither embeds a digest to the original data, nor sends any out-of band authentication information. Instead, our scheme is based on the timing correlation of data packets between the sender and the receiver. Particularly, the inter packet delays are utilized and some selected packet delays are slightly adjusted (in a range).

KEYWORDS: *Authentication, Wireless Sensor Networks*

Date of Submission: 25 February 2015 Date of Accepted: 20 March. 2015

I. INTRODUCTION

A Wireless Sensor Network (WSN**)** consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, enabling also to control the activity of the sensors. The development of wireless sensor networks and its applications are present in:

Military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and controlling the machine, health monitoring, and so on. A message authentication code (often MAC) is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. Integrity assurances detect accidental and intentional message changes, while authenticity assures and confirms the message origin.

To solve the scalability problem, a secret polynomial based message authentication scheme was introduced. The idea of this scheme is similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. This approach offers the information-theoretically and gives security for the shared secret key when the number of messages transmitted is less than the threshold. The intermediate nodes verify the authenticity of the message through a polynomial evaluation. However, when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken.

In this proposed method, Data-Transparent Authentication (DaTA) method is used without Communication Overhead and to authenticate data streams. This strategy neither embeds a digest to the original data, nor sends any out-of band verification information. Instead, this scheme is based on the timing correlation of data packets between the sender and the receiver. Particularly, the inter packet delays are utilized and some selected packet delays are slightly adjusted (in a range). The inter packet delay increase and decrease to represent different bits (0 or 1) transparently.

II. RELATED WORK

Statistical En-route Filtering of Injected False Data in Sensor Networks here present a Statistical En-route Filtering (SEF) mechanism that can detect and drop such false reports. SEF requires that each sensing report be validated by multiple keyed message authentication codes (MACs), each generated by a node that detects the same event. when the report is forwarded, each node along the way verifies the correctness of the MACs probabilistically and drops those with invalid MACs at earliest points. The sink node further filters out remaining false reports which escapes the en-route filtering. SEF exploits the network scale to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding nodes. It's used a Statistical En-route Filtering mechanism (SEF). The disadvantages are Sensor networks serving mission-critical applications are potential targets for malicious attacks. Although a number of recent research efforts have addressed security issues such as node authentication, data secrecy and integrity, they provide no protection against injected false sensing reports once any single node is compromised. The advantage of large scale by accumulating detecting power over data delivery paths: The more hops sensing reports need to travel through, the higher the probability that a forged report will be detected and dropped. Even when reports are forwarded through a small number of hops, SEF can still bring energy savings by detecting and dropping significant portions of forged reports. Given that real events may occur sporadically while forged reports can potentially be injected through compromised nodes by attackers at any rate, en-route filtering mechanisms such as SEF should be considered one of the necessary control mechanisms in any large scale networks.[1]

An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks present an interleaved hop-by-hop authentication scheme that guarantees that the base station will detect any injected false data packets when not more than a certain number 't' nodes are compromised. Further, our scheme provides an upper bound B for the number of hops that a false data packet could be forwarded before it is detected and dropped, given that there are up to 't' colluding compromised nodes. It's used a Interleaved hop-by-hop authentication scheme the limits are applied First, a node needs to establish 2(t + 1) pair wise keys. Second, for every data packet received, a node needs to compute up to 2(t + 1) MACs. In the original scheme, both the number of pair wise key establishment and MACs are bound by 4. Therefore, this variant scheme is preferred when t is small (e.g., t · 3). The advantages are First, it allows the en-route nodes to filter out false data packets immediately. Second, it does not require the authenticated neighbor knowledge; a node accepts a data packet only if it can verify t + 1 XMACs, whichever node sends the packet to it.[2]

Lightweight and Compromise-Resilient Message Authentication in Sensor Networks propose in this paper a novel message authentication approach which adopts a perturbed polynomial-based technique to simultaneously accomplish the goals of lightweight, resilience to a large number of node compromises, immediate authentication, scalability, and non-repudiation. Novel message authentication approaches are presented. If a message is tampered en route, it will be detected by the receiver. This method however is not effective due to the following reasons: First of all, it cannot authenticate messages that are multicast because, if one of the receivers is compromised, the intruder can use the secret key held by the compromised receiver to fake MACs for messages modified or injected by it itself to cheat other receivers. Secondly, the method only allows end-to-end message authentication while en-route forwarding nodes cannot authenticate pass by messages; as a result, the intruder may launch denial-of service attacks by repeatedly modifying messages or injecting false messages to deplete the communication resources of intermediate forwarding nodes. The advantages are Firstly adopt polynomials for message authentication, which provides higher adaptability than existing authentication techniques based on multiple MACs and at the same time, keeps the advantage of immediate authentication held by those techniques. Secondly, messages are authenticated and verified via evaluating polynomials, which incurs lower overhead than existing asymmetric cryptography-based authentication techniques such as digital signature. Thirdly, independent and random factors are employed to perturb polynomial shares (of a system-wide secret polynomial) that preloaded to individual nodes, which significantly increases the complexity for the intruder to break the secret polynomial, and therefore renders the proposed approach to be resilient to node compromises.[3]

Efficient Authentication and Signing of Multicast Streams over Lossy Channels propose two efficient schemes, TESLA and EMSS, for secure lossy multicast streams. TESLA, short for Timed Efficient Stream Loss-tolerant Authentication, offers sender authentication, strong loss robustness, high scalability, and minimal overhead, at the cost of loose initial time synchronization and slightly delayed authentication. EMSS, short for Efficient Multi-chained Stream Signature, provides non-repudiation of origin, high loss resistance, and low overhead, at the cost of slightly delayed verification. Two efficient schemes, TESLA and EMSS for secure lossy multicast streams. The biggest disadvantage, however, is that the entire stream of packets needs to be known in advance. The on-line scheme solves this problem through a regular signature of the initial packet and embedding the public key of a one-time signature in each packet, which is used to sign the subsequent packet. The limitation is again that this scheme is not robust against packet loss. In addition, the one-time signature communication overhead is substantial. The main advantage of this scheme is that any k0 out of the k packets need to arrive, which has a higher robustness in some circumstances than receiving 1 packet out of d in the basic scheme. First, the sender can predict how long a pre-computed key chain lasts, since the number of necessary keys is only time dependent and not on the number of packets sent. Second, the receiver can conveniently verify the security condition and the sender does not need to send its packets at specific intervals. Another advantage is that new receivers can easily join the group at any moment. A new group member only needs to synchronize its time with the sender and receive the interval parameters and a commitment to the key chain.[4]

Attacking Cryptographic Schemes Based on “Perturbation Polynomials” show attacks on several cryptographic schemes that have recently been proposed for achieving various security goals in sensor networks. Roughly speaking, these schemes all use “perturbation polynomials” to add “noise” to polynomial-based systems that offer information theoretic security, in an attempt to increase the resilience threshold while maintaining efficiency. show that the heuristic security arguments given for these modified schemes do not hold, and that they can be completely broken once allow even a slight extension of the parameters beyond those achieved by the underlying information-theoretic schemes. Perturbation polynomials are used. They have limited battery life, relatively low computational power, and limited memory. It’s describe efficient attacks against the schemes from, demonstrating that these scheme do not offer any better resilience than the original, information-theoretic schemes on which they are based.[5]

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key. A message can be signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in electronic mail" and electronic funds transfer" systems. Diffie and Hellman algorithm are used. The “key distribution problem." The problem is that before a private communication can begin, another private transaction is necessary to distribute corresponding encryption and decryption keys to the sender and receiver, respectively. Typically a private courier is used to carry a key from the sender to the receiver. Such a practice is not feasible if an electronic mail system is to be rapid and inexpensive. A public-key cryptosystem needs no private couriers; the keys can be distributed over the insecure communications channel. It provide efficient, high-quality encryption technique.[6]

Comparing Symmetric-key and Public-key based Security Schemes in Sensor Networks: A Case Study of User Access Control builds the user access control on commercial off-the-shelf sensor devices as a case study to show that the public-key scheme can be more advantageous in terms of the memory usage, message complexity, and security resilience. Meanwhile, our work also provides insights in integrating and designing public-key based security protocols for sensor networks. Elliptic curve cryptography algorithms are used. A main challenge of large scale sensor networks is the deployment of a practical and robust security mechanism to mitigate the security risks exposed to the unattended and resource constrained sensor devices. Motivated by the fact of insufficient hardware resources, a great deal of research has focused on the symmetric cryptography based solution for light-weight computation. The advantages are First, the sensors in proximity need to exchange pair wise keys for secure communications. Second, the user needs to get authenticated by the local sensors either for local sensor data access or for remote sensor data access. Third, the local sensors also need to help the user and the remote sensor build a pair wise key to achieve end-to-end security.[7]

Crowds: Anonymity for Web Transactions introduce a system called Crowds for protecting users' anonymity on the world- wide-web. Crowds, named for the notion of \blending into a crowd", operates by grouping users into a large and geographically diverse group (crowd) that collectively issues requests on behalf of its members. Web servers are unable to learn the true source of a request because it is equally likely to have originated from any member of the crowd, and even collaborating crowd members cannot distinguish the originator of a request from a member who is merely forwarding the request on behalf of another. Crowd’s mechanism are used. Lack of privacy in web and Encryption also does little to protect the privacy of the client from the server. A web server can record the Internet addresses at which its clients reside, the servers that referred the clients to it, and the times and frequencies of accesses by its clients. With additional effort, this information can be combined with other data to invade the privacy of clients even further. The advantages of more dynamic paths include the potential for better performance via load balancing among the crowd. In this section, however caution that dynamic paths tend to decrease the anonymity properties provided by the system against collaborating jondos.[8]

Security Arguments for Digital Signatures and Blind Signatures security arguments for a large class of known signature schemes. Moreover give for the rest time an argument for a very slight variation of the well known ElGamal signature scheme. In spite of the existential forgery of the original scheme prove that our variant resists existential forgeries even against an adaptively Chosen-message attack. This is provided that the discrete logarithm problem is hard to solve. ElGamal signature scheme algorithm are used. Prove that our variant resists existential forgeries even against an adaptively chosen-message attack. This is provided that the discrete logarithm problem is hard to solve. It's define an appropriate notion of security related to the setting of electronic cash. Then propose new schemes for which one can provide security arguments.[9]

Hop By Hop Message Authentication And Source Privacy In Wireless Sensor Networks

In the existing system is an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This MES scheme is secure against adaptive chosen-message attacks in the random oracle model. Existing scheme enables the in-between nodes to validate the message so that all dishonored message can be detected and dropped to preserve the sensor power. In the existing system provides source privacy but it didn't provide destination privacy.

Disadvantages

- Existing system didn't provide the source privacy
- Message authentication is not effectively provide

Message Authentication And Source Privacy Using BAC In Wireless Sensor Networks

In this propose method a novel method, Data-Transparent Authentication (DaTA) without Communication Overhead, to authenticate data streams. Our strategy neither embeds a digest to the original data, nor sends any out-of band authentication information. Instead, our scheme is based on the timing correlation of data packets between the sender and the receiver. Particularly, the inter packet delays are utilized and some selected packet delays are slightly adjusted (in a range). The inter packet delay increase and decrease represent different bits (0 or 1), and thus, transparently embed the digest.

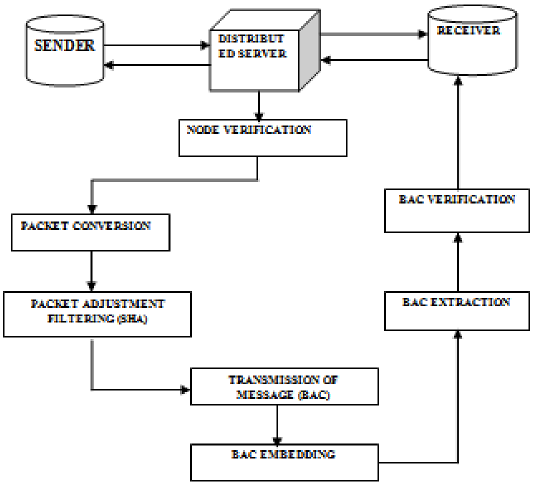


Fig 1: Architecture Diagram

Since limit the delay adjustment in a small range and the delay adjustment are not cumulative; the application's performance is hardly affected. Furthermore, our authentication strategy is no fragile, which can continuously authenticate the data stream even if a preceding data block is tampered with, and thus, provides stronger tamper detection capability at the block level. Modeling-based analysis reveals how the false positives and false negatives of our proposed scheme can be tuned. To evaluate our proposed scheme have implemented a prototype system and evaluated the system in an LAN and over the Internet. In the LAN, the experiments are performed under various network jitter patterns including normal and burst, and packet loss on both UDP- and TCP-based streams.

Advantages

- The results show that the proposed scheme is robust to packet loss and can succeed when various network jitter patterns exist.
- Little impact is found on the performance of the application. Over the Internet, the experiments are performed on nodes with 16-hop distance.

III. BAC ALGORITHM

AUTHENTICATION:

In Data, the authentication unit is a data block and the authentication code is generated based on the content of the data block, thus called Block Authentication Code (BAC). Data works as follows: At the sender side, the authentication information—BAC—is generated based on a selected hash function with the packet content and a commonly agreed key as the input. Based on the value of each bit (0/1) of BAC, some packets are scheduled to be sent out with additional delays.

At the receiver side, the receiver extracts the embedded BAC based on the relative packet delay and compares the extracted BAC with the BAC generated based on the received content for authentication. Thus, our proposed scheme consists of the BAC generation, BAC embedding/BAC extraction and BAC authentication. In this section describe the details of these components. Packet boundary recognition issue is discussed with regard to packet loss, packet fragmentation, and out-of-order delivery then. An algorithm for the computation of a free resolutions is called sequential if it uses the sequence of generators as first criterion for ordering the pair sets. This means, it extends recursively a resolution.

first $n-1$ generators to a resolution of n generators of a given ideal.

Algorithm : Sequential Search (A[1 .. n], key)

Input : An array A of n integers and an integer key

Output : A position of the key in the array (-1 if not found)

Project Description

Node Configuration Setting

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

Nodes Unique Identity

All the mobile nodes tend to have a unique id for its identification process, since the mobile nodes communicates with other nodes through its own network id. If any mobile node opted out of the network then the particular node should surrender its network id to the head node.

Message Exchange Process for Route Discovery

This module states a 4 step message exchange process i,e POLL, REPLY, REVEAL, REPORT. As soon the protocol executed the, POLL and REPLY messages are first broadcasted by Source and its neighbors, respectively. These messages are anonymous and take advantage of the broadcast nature of the wireless medium, allowing nodes to record reciprocal timing information without disclosing their identities

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

BAC Generation

The sender side, the authentication information BAC is generated based on a selected hash function with the packet content and a commonly agreed key as the input. Based on the value of each bit (0/1) of BAC, some packets are scheduled to be sent out with additional delays.

BAC Embedding/Extraction

After the BAC is generated, the next step is to embed the BAC. Different from existing strategies where the authentication information is sent out-of-band or embedded into the original data before data transmission, in DaTA, the BAC is embedded by adjusting the inter-packet delay. In the following context present how the BAC bits can be embedded and extracted without touching the content of the packet.

To extract the BAC, the receiver calculates Yr; d as it receives the data packets. To extract an embedded bit, the receiver checks whether Yr; d is less than or greater than 0. The extraction of embedded binary bit is 1 if the value of Yr;d is greater than 0, or 0 if the value of Yr;d is less than or equal to 0. It is easy to see that probability of correct extraction is always greater than that of wrong extraction.

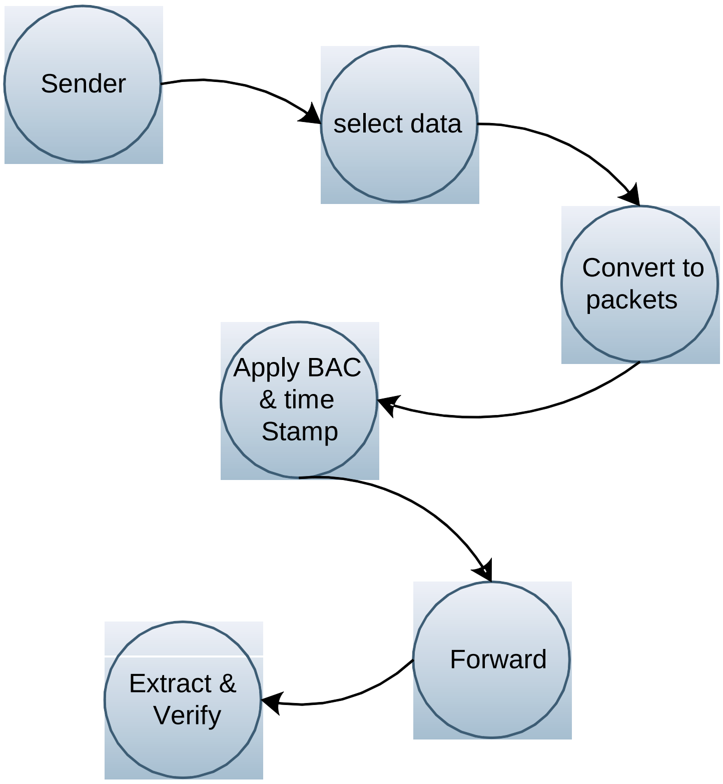
BAC Authentication

With the extracted BAC bits and received data packets, the receiver applies the same hash function (H) on the received data packets with the same secret key (k) to generate the content-based BAC following the same procedure used for BAC generation at the sender side. Then, the extracted BAC is compared with the generated BAC.The comparisons consist of two parts: the first part is on the first n bits, while the second is on the rest f 0 bits.

Comparison Graph

The performance analysis of the existing and proposed work is examined through graphical analysis. Compare the time, throughput and packet delivery ratio.

Extract And Verify The Packets



First users select the data to send a particular person or receiver; then forwarding contents are converted into packets. After converting the packets, applying BAC operations. First step of the BAC is generated based on a selected hash function with the packet content and a commonly agreed key as the input. Second step is to embed the BAC, by adjusting the inter-packet delay. Forward the packets to the receiver. Third step is BAC authentication the receiver applies the same hash function (H) on the received data packets with the same secret key (k) to generate the content.

CONCLUSION

In the proposed work a new scheme by adjusting packet timing (delay) to authenticate the data stream. Thus, authentication is done without changing the original packet content and without sending additional authentication information. Extensive experiments are conducted locally and over the Internet based on an implemented prototype system and which gives robustness.

FUTURE WORK

In this project this scheme is applicable for uni-casting only. In future it can be extended for multicasting and broadcasting.

REFERENCES

[1]. F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, Mar. 2004.

[2]. S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-By- Hop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004

[3]. W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.

[4]. A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," Proc. IEEE Symp. Security and Privacy May 2000.

[5]. M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.

[6]. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[7]. H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor".

[8]. Michael K. Reiter and Aviel D. Rubin "Crowds:Anonymity for Web Transactions".

[9]. David Pointcheval and Jacques Ster "Security Arguments for Digital Signatures and Blind Signatures".