Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

PROVIDING MESSAGE AUTHENTICATION AND SOURCE PROTECTION AGAINST DATA IN SENSOR NETWORKS

L.Naga Keerthi[1], V.Sreenatha Sarma[2]
[1] *M.Tech(CSE), Audisankara college of engineering and technology ,Gudur,*
[2] *M.Tech(CSE), Audisankara college of engineering and technology,Gudur*

Abstract- While enabling intermediate node authentication,a scalable authentication scheme is proposed based on elliptic curve cryptography.It allows any node to transmit unlimited number of messages without suffering from threshold problem and also provides source privacy.In this paper we propose a Data Transparent Authentication (DATA) to validate message without communication overhead.This scheme requires no change to original data and there is no communication overhead.This scheme is based on timing correlation between sender and receiver.
Keywords-hop-by-hop confirmation, symmetric-key cryptosystem,asymmetric-key cryptosystem, source protection, remote sensor systems (WSNs), decentralized control

I.INTRODUCTION

Message authentication plays a key role in removing unauthorized and ruined messages from being forwarded in networks.Many schemes were proposed to provide message authenticity and integrity.Authenticity checks whether a received message is sent by the correct node and integrity is to confirm whether the message has been modified or not.

To take care of the scalability problem, a secret polynomial based message authentication scheme is presented. This plan is like threshold secret sharing, where the threshold is controlled by the level of the polynomial. This offers data theoretic security of the common secret key when the quantity of messages transmitted is not exactly the limit.The intermediate nodes check the credibility of the message through a polynomial evaluation. However, at the point when the quantity of messages transmitted is bigger than the limit, the polynomial can be completely recouped and the framework is totally broken.

In this proposed system[1][2], Data Transparent Authentication (DATA) strategy is utilized without communication overhead and to confirm information streams. This technique neither implants a summary to the first information, nor sends any out-of band check data. Rather, this plan is based on the timing connection of information between the sender and the recipient[3][4].

II.LITERATURE SURVEY

A remote sensor system (WSN) of spatially appropriated self-sufficient sensors to screen physical or ecological conditions, for example, temperature, sound, weight, etc and to cooperatively pass their data through the network to a main location.Wireless sensor systems was utilized by military applications, for example, war zone reconnaissance.Based on this wireless sensor,networks consists of two types of attacks launched by the adversaries:

A.Passive Attacks:

Through passive attacks, the adversaries can attack the IP address of the network and perform traffic analysis.

B.Active Attacks:

Active attacks can only be launched from the compromised sensor nodes. Once the sensor nodes are compromised, the adversaries will obtain all the information stored in the compromised node.The adversaries attack the node directly and change the contents of the message.

Factual En-route Filtering of Injected False Data in Sensor systems here present a Statistical Enroute Filtering (SEF) mechanism that can identify and drop false reports[5]. SEF obliges that every detecting report be accepted by different keyed message validation codes (MACs). At the point when the report is sent, every hub along the way confirms the accuracy of the MACs probabilistically and drops invalid MACs. The sink hub further sift through staying false reports.The disadvantages are Sensor systems serving mission-discriminating applications are potential focuses for malignant assaults. In spite of the fact that examination endeavors have tended to security issues such as node validation, data secrecy and integrity, they give no protection against injected false detecting reports once any single hub is traded off. The benefit of expansive scale by accumulating detecting power over information delivery paths.

An interleaved Hop-by-Hop Authentication Scheme for separating of Injected False Data in Sensor Networks presents an interleaved hop-by-hop validation scheme that ensures that the base station will recognize any infused false information packets when not more than a specific number "t" hubs are bargained. Hop-by-hop authentication scheme is implemented for perfect authentication.In militating application we always need to monitor the opponents activity [6].These can be achieved by clustering certain group of nodes for end-to-end transport protocols such as TCP and we can also create a base station in a secure location to control the sensor and to collect the data .A hacker may compromised sensor node and then use the same node to inject the false or wrong data to network. Here author focuses his work towards the false injection attacks. According to this,base station is responsible for enabling the authenticity of report. Scheme filter out the false injected packet into the network by compromised node before reaching towards the base station. Author's main intention to provide the security while transmission of packets.

Attacking cryptographic scheme show attacks on several cryptographic that have recently been proposed for achieving different security goals in sensor networks.These schemes use "perturbation polynomials" to include "noise" to polynomial-based systems that offer information theoretic security while maintaining efficiency[7]. They demonstrate that the heuristic security contentions given for these changed plans don't hold, and that they can be totally broken once we permit even a slight expansion of the parameters past those accomplished by the fundamental data theoretic plans.

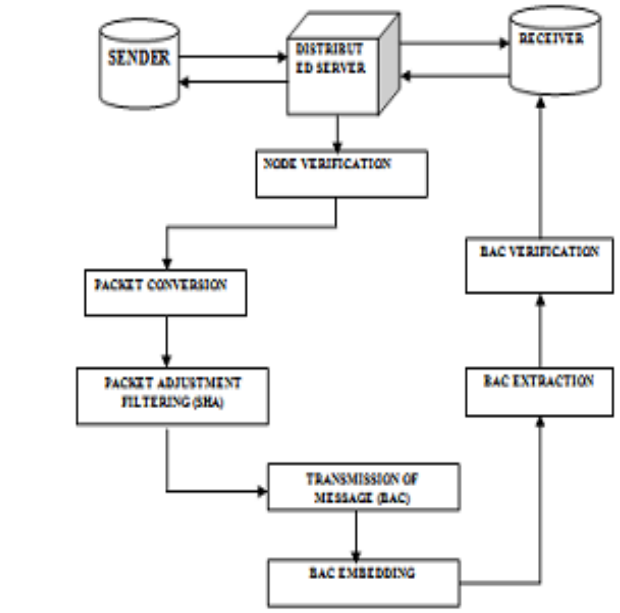
Hop by hop message authentication and source privacy in wireless sensor networks is an genuinely secure and efficient Source Anonymous Message Authentication (SAMA) scheme based on the optimal Modified ElGamal Signature (MES) scheme on elliptic curves. This MES arrangement is secure against versatile chosen message assaults in the arbitrary prophet model. Existing plan empowers the intermediate nodes to approve the message with the goal that all dishonored message can be distinguished and dropped to safeguard the sensor power.The current system provides source protection.

III.ACTUAL WORK

In this propose strategy a novel technique, Data-Transparent Authentication (DATA) without communication overhead is used.Our system neither implants a condensation to the first information, nor sends any out-of band verification data. Instead, proposed plan is based on the timing relationship of information between the sender and the receiver. Especially, the inter packet delays are used and some chosen packet delays are slightly balanced. The inter packet delay expand and diminish to represent diverse bits (0 or 1) transparently.

A. Basic DATA(data transparent authentication)

In DATA ,authentication code is generated on the content of data block called Block Authentication Code(BAC).At sender, BAC is generated based on selected hash function. Based on the value of each bit(0/1),some packets are scheduled to sent out with additional delays. The receiver extracts BAC based on packet delay and compare extracted BAC with BAC generated.



\

Fig: Architecture diagram

B.BAC Generation

The sender side, the verification data BAC is created taking into account based on selected hash function and an ordinarily used concurred key as input. Based on estimation of every bit (0/1) of BAC, some bundles are planned to be conveyed with extra defers.

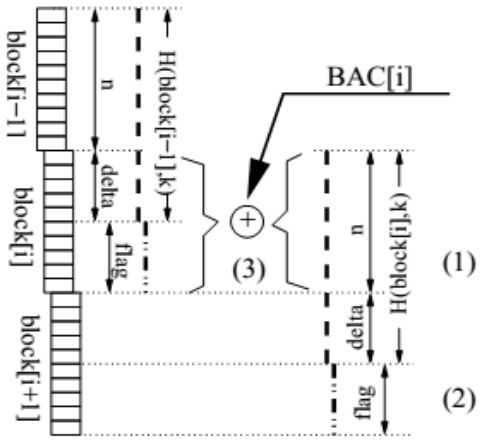


Fig: Generating block authentication code

C.BAC Embedding and Extraction

Once the BAC has been produced, it should be transferred to the recipient of the gushing information so that the spilling information can be confirmed. Dissimilar to most existing spilling information validation approaches, which either exchange the confirmation code by means of out of band correspondence or insert the verification code into the first information content, DaTA influence the methodology utilized as a part of to implant the BAC into the between parcel timing.

Assume the streaming data flow has m packets P1, . . . , Pm with time stamps t1, . . . , tm, respectively. To embed one bit, we first independently and randomly choose 2r (r > 0 is the redundancy used for embedding the bit) distinct packets:Pz1, . . . , Pz2r ($1 \le zk \le m - 1$), and create 2r packet pairs: hPzk, Pzk+1i ($d \ge 1$, k = 1, . . . , 2r).

We are interested in the 2r IPDs (Inter-Packet Delay) between Pzk+1 and Pzk

ipdzk = tzk+1 − tzk, (k = 1, . . . , 2r).

We randomly partition the 2r IPDs into 2 distinct groups of equal size, and verify that each IPD has equal probability. We utilize ipd1,k and ipd2,k (k = 1, . . . , r) to represent the IPDs in group 1 and group2 . Since each IPD has equal probability, IPDs in group 1 and group 2 are symmetric.

D.BAC Authentication

With the separated BAC bits and got information packets, the receiver applies the same hash function(H) on the got information bundles with the same secret key (k) to produce the content based BAC taking after the same system utilized for BAC generation at the sender side . At that point the removed BAC is compared with the generated BAC. The correlations comprise of two sections: the first part is on the first δ bits, while the second is on the rest f (= n − δ) b. Comparison result is as follows:

case number	δ bits	$n-\delta = f$ bits	Current Data Block	Other Implications
1	match	match	true	None
2	match	mis-match	false	current data block changed
3	mis-match	match	true	preceding data block loss/deletion or alteration
4	mis-match	mis-match	false	current data block changed

IV.CONCLUSION

In this paper,we proposed a new scheme by adjusting packet timing to authenticate data and confirmation is done without changing the original packet content. Extensive experiments are conducted locally and which gives robustness.

V.REFERENCES

[1] "National hurricane center," http://www.nhc.noaa.gov/.
[2] "National maritime and environmental administration, "http://www.nesdis.noaa.gov/.
[3] CIBER Stock Quote & Chart/Share Price, " http://www.advfn.com/.
[4] Data straight forward validation,"cs.gmu.edu/~sachem/distributions/information secure comm".
[5] F. Yes, H. Lou, S. Lu, and L. Zhang, “Statistical En-Route Filtering of Injected False Data in Sensor Networks,” Proc. IEEE INFOCOM, Mar. 2004.
[6] S. Zhu, S. Seta, 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.
[7] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, “Attacking Cryptographic Schemes Based on ‘Perturbation Polynomials’,” Report 2009/098, http://eprint.iacr.org/, 2009.