International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7, Issue-6, March 2019

Message Authentication using Threshold Blockchain in VANET

N Sushmetha, S Vairamuthu

Abstract*: The Over the past decade, metropolitan cities have witnessed a hive of activity leading to sustained levels of air pollution. The five prime pollutants are Carbon Monoxide (CO), Particulate Matter (PM), Nitrogen oxides, Sulphur dioxide (SO2) and ozone (O3). The air contaminates when these pollutants commingle, making it lethal to mankind. The inception of blockchain and VANET have paved its way to a variety of prospects including medicine, economics, internet of things and software engineering to name a few. The data collected from humans close to smart vehicles, connected to the Wireless Body Sensor Network (WBSN), is sent to the assessing module. The system learns nothing about the data being processed. In this paper blockchain with an additional layer of security has been proposed for an infrastructure less environment. In order to address one among many risks involved in the block chain framework, threshold cryptography scheme has been included to further suite ad hoc environment. The secret key is not trusted with any particular node but distributed.

***Index Terms*: Blockchain, threshold, Ad Hoc, Authentication**

I. INTRODUCTION

There is a growing need to perform authentication especially in mobile client-server architecture where the nodes rapidly migrate from one network to another. For the sake of visual acuity, a group of nodes in network A may have a cluster head and a roadside unit (RSU) to authenticate from time-to-time. Nevertheless, when a node from network A enters the boundary of another network there is a desperate need to authorize and reauthenticate, such that it complies with the security policies of the defined framework. In such a dynamic topology involving public-private key mechanism huge memory overhead is incurred by the Roadside Unit and the mobile nodes and the necessity to re-authenticate frequently. Such Ad Hoc infrastructure demands the address various security issues [1] . Na Ruan et al have proposed addresses the vulnerabilities associated with a semi-trusted road side unit when compromised using a key management scheme based on threshold ElGamal cryptography [2].

Blockchain provide a decentralized framework in which the authority to perform addition or modification at any level is distributed [3]. Retroactively relying on legacy with a malicious intent to carry out any attack is partially eliminated since unlike traditional methods of authentication it remains impossible to roll back any communication or transaction, thus protecting the legitimacy intact. This briefly eliminated a consensus mechanism involving a trusted third party thereby the risk of double spending though not completely. This work addresses risk associated with the strength of a single miner's hash value(51 % vulnerability) which is viewed common to both blockchain version 1.0 and 2.0 [3].

The threshold consensus mechanism proposes distributing the authority across nodes in a network satisfying two major conditions: (1) at any point in time a plowshare of nodes can pave to reconstruct provided it meets the threshold. (2) shares under the thresholds yields no information [4]. There have been various advancements in field of two factor authentication in the past decade. The various shades of two-factors suffer from one major drawback which is impersonation attack [5].

II. LITERATURE SURVEY

In [2] Na Ruan et al have proposed a threshold key management scheme to address the vulnerability associated with Road Side Units. The architecture includes three elements namely On Board Units, Distributed Road Side Unit and the Certificate Authority. It addresses the need to distribute the secret key among nodes to facilitate easy revocation. CA has the top most security privilege followed by DRSU and OBUs. The vulnerability lies in the second level and hence threshold ElGamal is added to this layer. However this incurs a lot of processing overhead. Therefore threshold mechanism is not suitable for commercial platforms since unlike military applications tolerant of selfish nodes, commercial employ conservation mechanisms which leads to data loss [1]. This has been addressed by a lightweight authentication protocol and the interleaved message authentication mechanisms [6].In order the vulnerabilities associated with a shared multi party wallet, Oliver stated the benefits of a crypto-processor that generates private key having tamper secure OS. This is called the hardware security module(HSM) [7].Though the device is protected from physical tampering by a casing and privacy key is wiped off in case of breach it still suffers from the need to be stored privately from unauthorized access. Two factor authentication employed using hash key, RSA algorithm and smart card though proves to be defensive against malicious attacks like replay, insider, impersonation thereby preserving anonymity suffers from the one major drawback of protecting the physical device(smart card) [5][8].

Revised Manuscript Received on 30 March 2019.
* Correspondence Author
N.Sushmetha*, School of Computer Science and Engineering,VIT University, Vellore, India
S.Vairamuthu, School of Computer Science and Engineering,VIT University, Vellore, India

This being a highly sensitive method of authentication proves to be vulnerable with even slight variations. The de synchronization attack addressed by Wang et al however suffers from forward secrecy [8]. Protection against other malicious attacks has been provided with no additional computational cost . A three factor authentication scheme proposed by Qi Xie et al for mobile network uses a random nonce in addition to the elliptic cryptography scheme to overcome the impersonation attack [9] . However the fact that mobile network can be enhanced with a threshold system to the ad hoc environment thereby eliminating a centralized authority.

III. PROPOSED METHOD

In the proposed work, an attempt to extend the multi factor security involving threshold scheme of blockchain to an Ad Hoc environment has been made. Association of three attributes makes the blockchain framework which is (1) hash of the previous block (2) timestamp (3) transaction data. The system conforms to the basic blockchain framework with the threshold flavour eliminating the risk of single point failure. The network architecture snatches the authority of a trusted cluster head. No node is trusted more than any other. The underlying concept in blockchain is public key cryptography. A long random string of digits called the address of the blocks forms the public key. This is used to identify the nodes in the network uniquely. Also the address does not reflect the real world identity and every time a node tries to exchange data or communicate, be it with the central unit or other nodes it attributes to the creation of a new block in the hierarchy. The private key is distributed among the nodes such that a threshold t out of n nodes is needed for authentication or communication between networks. It is an infrastructure less environment and hence the dynamic nature is addressed by multi factor consensus. There is no hierarchy privilege awarded to nodes. The mica mote is a sensor node part of the Wireless Body Sensor Network (WBSN) capable of gathering information and processing. The gas level breathed by the user is recorded and sent to the vehicle. It is important that at least three gases be sent.

IV. DATASET

The real time values of three out of eight pollutants were obtained which are monitored by the government of India. The values are extracted using the xmlstarlet command line.

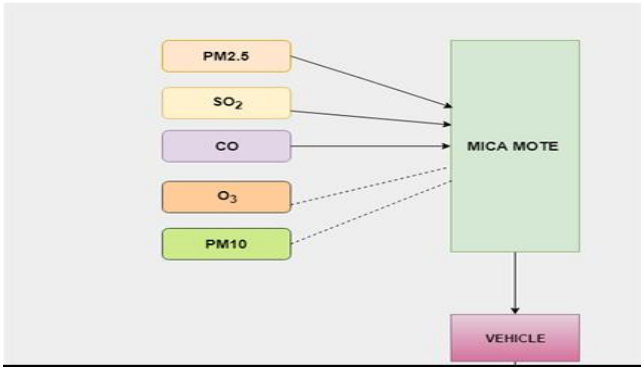

Fig 1: Communication Model

Fig 2. Sample data

V. IMPLMENTATION

Threshold Signature underlies elliptic curve digital signature algorithm (ECDSA) by distributing the redeeming power to a constant number of shares not bound by the address. Without loss of generality, in a group of n nodes there maybe q deceptions such that (n>= 2q+1) and a threshold of q+1 is a fundamental necessity to redeem the authentication. That is to say, less than q+1 cannot proceed any further.

a) Each of the n nodes compute c= SHA1(M). The value of c is translated to corresponding integer in ANSI X9.62.

b) Nodes computes the individual share of the secret using the algorithm proposed in [10]. It offers lower computation cost compared to the legacy of secret sharing algorithms.

c) Node j computes the Langrange fundamental polynomial $d_j = \prod_{k \neq j, k \in D} \frac{k}{k-j}$.

d) Node k computes $x_j = d_j t_j$ broadcasts $U_j = x_j G$.

e) Nodes compute $(e_1, f_1) = tG = \sum_{j \in D} U_j$

f) Translate e_1 to an integer format in ANSI X9.62. Compute $p = e_1 \bmod n$. If $p = 0$, go to step 2.

g) Nodes run the secure reciprocal protocol given in [10].

h) Nodes then compute portions of $y = bt^{-1}$ over a degree l polynomial by multiplying their shares of b and t^{-1} and running the secure degree reduction protocol.

i) Each Node computes the share
$r_i = t_j^{-1} \cdot c + p \cdot y_j = t_j^{-1} \cdot c + p(b_j \cdot t_j^{-1}) = t_j^{-1}(c + b_j p)$

j) Nodes interpolate their shares of r to recover
$r = t^{-1}(c + bp)$. 0 If $r=0$, go to step 2.

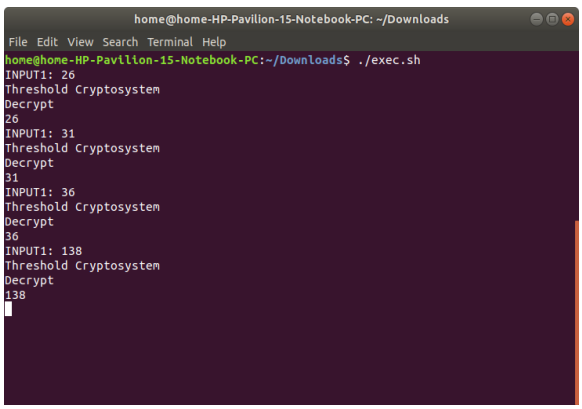

Fig 3: Threshold ECDSA implementation

k) The signature for *M* using key *b* is the pair *(p,r).*

Threshold ECDSA is implemented in python environment. The threshold number of nodes and the existing participants in the network is given as input. The reconstructed private key is generated and the output is verified (Fig 3).

VI. CONCLUSION

In this paper, message authentication using a threshold scheme with less computational power is performed to suite the ad hoc environment. Unlike message authentication using multi signature approach which allows at least on player to redeem all the other keys, this setup offers better security. The distributed and decentralized nature of the blockchain facilitates authentication of a new node in ad hoc environment. The selection of the threshold is however done in an interactive fashion which allows the new node to not decide the threshold but also to verify the share of private key. Thus the threshold blockchain offers flexibility, confidentiality and scalability with user anonymity.

REFERENCES

1. M. A. Azer, S. M. El-Kassas, and M. S. El-Soudani, "Threshold cryptography and authentication in ad hoc networks survey and challenges," in *Systems and Networks Communications, 2007. ICSNC 2007. Second International Conference on*, 2007, p. 5.
2. N. Ruan, T. Nishide, and Y. Hori, "Threshold ElGamal-based key management scheme for distributed RSUs in VANET," in *Mobile and Wireless Networking (iCOST), 2011 International Conference on Selected Topics in*, 2011, pp. 133–138.
3. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Futur. Gener. Comput. Syst.*, 2017.
4. S. Goldfeder, J. Bonneau, J. A. Kroll, and E. W. Felten, "Securing bitcoin wallets via threshold signatures," 2014.
5. P. Chandrakar and H. Om, "RSA based two-factor remote user authentication scheme with user anonymity," *Procedia Comput. Sci.*, vol. 70, pp. 318–324, 2015.
6. B. Lu and U. W. Pooch, "A lightweight authentication protocol for mobile ad hoc networks," in *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on*, 2005, vol. 2, pp. 546–551.
7. O. Boireau, "Securing the blockchain against hackers," *Netw. Secur.*, vol. 2018, no. 1, pp. 8–11, 2018.
8. D. Wang, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity," *Inf. Sci. (Ny).*, vol. 321, pp. 162–178, 2015.
9. Q. Xie, Z. Tang, and K. Chen, "Cryptanalysis and improvement on anonymous three-factor authentication scheme for mobile networks," *Comput. Electr. Eng.*, vol. 59, pp. 218–230, 2017.
10. X. Li and M. He, "A protocol of member-join in a secret sharing scheme," in *International Conference on Information Security Practice and Experience*, 2006, pp. 134–141.

AUTHORS PROFILE

N Sushmetha is currently pursuing her M.Tech in CSE with specialisation in information security at Vellore Institute of technology.

Dr. S Vairamuthu is currently associated with Department of Software Systems, School of Computer Science and Engineering of Vellore Institute of Technology. His current areas of interest include: Human computer Interaction, Information Security, Data Analytics and IoT. He has good publications in reputed peer reviewed journals and conferences of international repute.