SUMMARY REPORT 2

Hadi Jibbawi

BBAAS: Blockchain-Based Anonymous Authentication Scheme for Providing Secure Communication in VANETs

- **Proposed System Overview:**
  - Trusted Authority: vehicles submit its original credentials to TA. TA generates public/private key for vehicle and calculates an authentication code.

    Note: public/private keys and authentication code are the metrics used to track malicious vehicles with the assistance of RSUs.
  - Roadside units (RSU): verify and anonymously authenticate all the broadcasted transactions of the vehicles, and add new block to blockchain.
  - Vehicles: Stores the secret and unique credentials in the on-board unit which are used to secure communication and computation operations.
- **Security Analysis:**
  - Metrics: Various security attacks, anonymity, and forward secrecy.
  - Anonymity: The real identities are stored only at the trust authority. So, the scheme achieves authentication with anonymity.
  - Replay Attack and Man-in-the-Middle Attack: delay in messages turns timestamp invalid. Each connection between vehicle and RSU is established via s new generated secret key based on the private credentials, so not encrypted messages will be discarded by the RSU. Authentication code is generated automatically and updated immediately in the blockchain by the TA. Hence, scheme is secure in terms of Replay and Man-in-the-Middle attacks.
  - Message Modification Attack: integrity of messages is preserved by blockchain through the block's hashes.
- **Performance Analysis:**
  - Metrics: storage cost, communicational cost, and computational cost.
  - Storage cost: Generally, the storage cost in blockchain is considered an important parameter in RSU and TA.

  - Computational Cost:

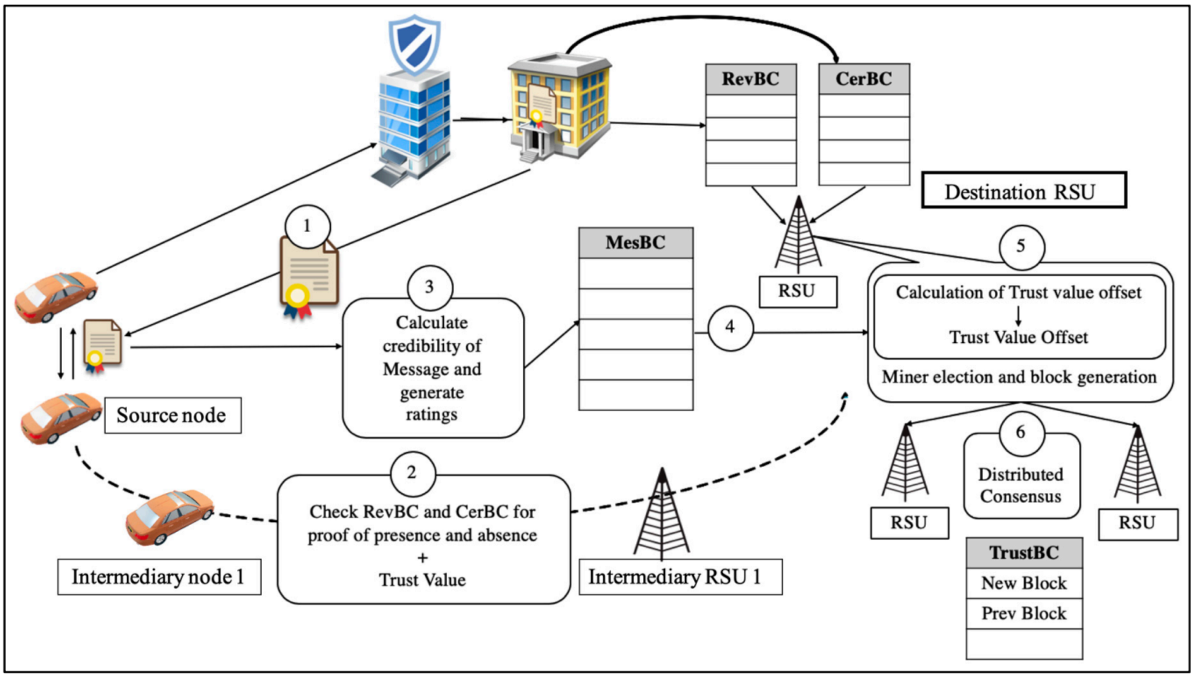
BBAAS	Other existing approaches
490 ms for anonymous authentication of 100 user	More than 580 ms for anonymous authentication of 100 user

  - Communicational Cost:

BBAAS authentication phase (bits)	BBAAS handover authentication phase (bits)	Other existing approaches (bits)
2048	1096	More than 4096

Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET

- **Proposal:** a secure trust-based modal that utilizes blockchain technology in order to mitigate medium access control (MAC) layer threats such as DoS attack and data modifications attack.
- **Design of the proposed architecture:**
    - Blockchain is implemented on the MAC layer (layer 2).
    - Signature less public key infrastructure is integrated to the solution to preserve the privacy of the users in the network.


RevBC
CerBC
Destination RSU
1
MesBC
RSU
5
3
Calculate credibility of Message and generate ratings
4
Calculation of Trust value offset
Trust Value Offset
Miner election and block generation
Source node
2
Check RevBC and CerBC for proof of presence and absence
+
Trust Value
6
Distributed Consensus
RSU
RSU
Intermediary node 1
Intermediary RSU 1
TrustBC
New Block
Prev Block

RevBC: Revoked Blockchain, CerBC: Certificate Blockchain, MesBC: Message Blockchain

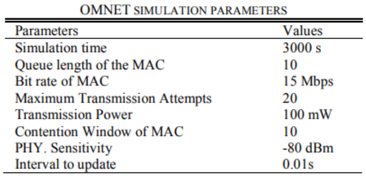
- **Simulation:**
    - Cases: with and without DoS Attack.
    - Compared with existing protocols: authentication based on smart card (ASC); lightweight authentication and key agreement protocol (LAKAP); hybrid approach for privacy-preserving authentication scheme (HEPPA); efficient, scalable, and privacy-preserving authentication (ESPA); and secure privacy-preserving authentication with cuckoo filter (SPACF).
    - Simulation Tool: Vein
    - Performance Analysis:
        - Packet Delivery Ratio (PDR):
            - Without DoS: higher PDR with difference more than 2.4% from existing solutions
            - With DoS: higher PDR with difference more than 17.5% from existing solutions
        - End-to-End Delay:
            - Without DoS: lower end-to-end delay with difference between 0.08s and 0.3s from existing solutions
            - With DoS: lower end-to-end delay with difference between 0.22s and 0.39s from existing solutions
        - Transmission Overhead: lower transmission overhead compared to the benchmark protocols because of its implementation of a signature less public key

        infrastructure authentication technique to maintain a lighter and shorter packet header
    - Computational Cost: lower computational cost with difference between 0.19ms and 0.49 ms from existing solutions

- Security Analysis:
    - Uniqueness of blockchain makes data hard to be overwritten, deleted or modified.
    - Single point of failure is not possible due to decentralized trust across network.
    - Privacy protection: users can be part of the network without revealing their real identity.
    - Hashing protocol (based on MAC address, data integrity and digital signatures) makes data accurate and reliable.
    - Proposed mechanism can ensure confidentiality, integrity, availability, and non-repudiation. In terms of confidentiality, the use of elliptic curve cryptography encryption for all V2V and V2I communications is capable of mitigating data modification attack, impersonation attack. From an integrity point of view, each communication includes a hash and a timestamp of all other fields contained in the communication. Each block is linked with the previous hash; hence all communications are chained together, making it impossible for Sybil and replay attacks to occur. Last but not least, based on the experiment done, denial of service attacks does not seem to affect VANET, as the trust management algorithm only allows legitimate nodes to participate in the network and isolate possible malicious nodes before they cause irregularities in the network. Moreover, the decentralized nature of the blockchain architecture makes the VANET prone to severe downtime in the case of other external issues, securing the network availability at all times. In our future work, formal methods will be used to conduct extensive security analysis.

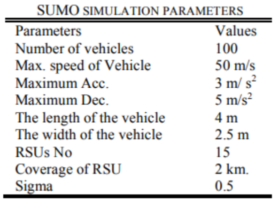
A Privacy-Preservation Framework based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET

- **Proposal:** a biometrics blockchain (BBC) framework to secure data sharing among vehicles in VANET and to retain statuary data in a conventional and trusted system.
- **Framework Components:**
  - Trusted Authority (TA): initializes system, deploys smart contracts, registers vehicles and revokes registrations.
  - Motor Vehicle Department (MVD): vehicle registration, maintaining vehicle records, authorizes TA to issue certificates and public keys to the vehicles after verification process is completed from MVD.
  - Vehicle
  - RoadSide Unit (RSU)
  - Blockchain: responsible for secure handling of the transactions (safety messages) exchanged by vehicles across the network.
- **Biometrics based Authentication:**
  - OBU have finger print scanner which scans the finger print of the driver and send it with the driver's information needed to register at TA.
  - Registration begins with obtaining real identity of the vehicle from the MVD, and sending the biometric data of the vehicle's authorized user and vehicle ID to the TA. After verification, TA generates certificate holding pair of keys. After that vehicle can join the blockchain
- **Simulation**: Using OMNeT++, Veins, and SUMO.
  - Parameters:



OMNET SIMULATION PARAMETERS

Parameters	Values
Simulation time	3000 s
Queue length of the MAC	10
Bit rate of MAC	15 Mbps
Maximum Transmission Attempts	20
Transmission Power	100 mW
Contention Window of MAC	10
PHY. Sensitivity	-80 dBm
Interval to update	0.01s



SUMO SIMULATION PARAMETERS

Parameters	Values
Number of vehicles	100
Max. speed of Vehicle	50 m/s
Maximum Acc.	3 m/ s^2
Maximum Dec.	5 m/s^2
The length of the vehicle	4 m
The width of the vehicle	2.5 m
RSUs No	15
Coverage of RSU	2 km.
Sigma	0.5

  - Compared Existing solutions: BC-VANET, ASC and LAKAP
  - Performance Analysis:

	Without DoS		With DoS	
	Framework	Existing	Framework	Existing
Packet Delivery Rate	0.99	0.9-0.98	0.96	0.7-0.94
Computational Cost (20 vehicles)	0.1 ms	0.13 ms- 4 ms	0.1 ms	0.13 ms- 4 ms

  - Security Analysis:
    - Secure Registration: ensures security using public and private keys. The keys are stored in the OBU which is a tamper proof memory. The vehicle is registered only when the registration data is verified with MVD. The data is sent to network by signing with private key of the vehicle.
    - Data Integrity: authentication and data are protected by hash function, signature and match functions.
    - Privacy Preservation and Traceability: real identity is not revealed to anyone, and data is traceable by the blockchain when any malicious activity occurs.

Blockchain-Based Pseudonym Management Scheme for Vehicular Communication

- **Proposal:** a lightweight pseudonym management scheme for vehicular authentication using blockchain.
- **Simulation:**
    - SUMO: to generate the vehicle traffic
    - OMNET++ with Veins: to simulate the network communication
    - Permissioned blockchain framework was implemented using hyperledger composer.
- **Analysis:**
    - Reduce authentication delay and computation overhead on vehicle OBUs.
    - Increased message exchange with the RSUs.
    - Effective under low to moderate channel loads.
    - Recommended that additional congestion control mechanisms should be implemented for higher loads.

A Secured Message Transmission Protocol for Vehicular Ad Hoc Networks

- **Proposed system structure:**
    - Vehicles of same direction are considered as clusters
    - In the cluster, one vehicle is elected as Cluster Head (CH) and others become Cluster Member (CM)
    - Cluster is a centralized system where the NSMTs between CMs are handled by the CH as an access point.
    - Every cluster owns a blockchain to store the safety messages.
- **Experiment:**
    - Blockchain server: Ganache Test Server
    - Deployment of smart contracts and transactions execution: Rinkeby Ethereum Testnet.
    - Safety Messages transmitted by internet.
    - SCB-MAC (internal network) for non-safety messages transmission
- **Performance Analysis:**
    - NSMT maximum throughput of 12Mbps. (Some previous solutions 1.1-11 Mbps
    - Full network is for non-safety messages only so it results in throughput increment
- **Security Analysis:**
    - Secure Authentication and Non-Repudiation: using the PKI based digital **signature** method.
    - Privacy Preservation: real identity is stored only in the CA and not used in communication
    - Security, Integrity and Confidentiality of messages: SMTs are encrypted by RSA-1024 cryptographic algorithm. And the blockchain checks for the integrity of message by its hashing method.
    - DDoS attack: blockchain never accepts unauthorized entity to perform any operation.

DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts

- **Proposed Architecture**
    - Vehicles, RSUs, Blockchain
    - SC1: public smart contract that interacts with the RSUs and ensures that the data generated from vehicles is coming from trusted origin.
    - SC2: private smart contract responsible for storing and retrieving data from blockchain.
    - Every node in DrivMan has a blockchain account
    - DrivMan integrates with PUF which gives a unique crypto ID.
- **Evaluation:**
    - Storage overhead: considering that new block is generated each 10 sec, storage overhead for one blockchain is 1602 MB/year.
    - Time consumption: time: time for SHA-256 is less than 0.01ms per 1 KB of input
    - Data tamper proofed: due to the blockchain mechanism
    - Secret response of an vehicle cannot be revealed: every vehicle has its own PUF
    - Public key of vehicles cannot be correlated: RSUs (CA) generates the public keys of vehicles randomly.