Application and architecture for localization in a trustful iot environment with permissioned blockchain support

BASE

In this report is proposed an iot and blockchain architecture to establish a position of a target in trustful environment, without disclosing the information of devices and position data to no authorized user.

This research is based on the paper “A Trust Architecture for Blockchain in IoT” (1).

In that paper is presented a layered architecture for improving the end-to-end trust of sensors data.

The main component of the structure are the devices, the gateways and blockchain. The devices are the means to capture some data from the environment and send them to apposite gateway. The gateways evaluate the trust of devices and insert the data in the blockchain. Between gateways it is evaluated the reputation of gateways. The blockchain maintains secure and untempered the data.

The architecture evaluates the trustworthiness of sensor observations at the data layer and adapts block verification at the blockchain layer through the proposed data trust and gateway reputation modules. Then, proposed system is evaluated in a localization scenario.

The trust layer proposed consists in two key modules: (1) the data trust module; and (2) the gateway reputation module. The data trust module calculates the trust given to an observation from a device. This trust consists in three elements: Confidence of the data source (conf); Evidence from other observations (sens); Reputation of the data source (rep).

The confidence of a device observation is the level of trust a device gives to its observation. In the paper case is the signal power received from a target by a device.

The evidence from other observations is a value that represents the level of support neighbor devices give to an observation of a device. For example, in the paper case, the value can be the similarity of the distances value calculated from other devices with the distance calculated by a specific device.

The reputation of the data source is a value that evolve during the life of system and it depends on behavior of the device. If the device behaves maliciously the reputation decreases, contrary the reputation increases.

The trust of a device is calculated through this formula: Trust = conf \* sens \* rep.

Instead, the gateway reputation consists in module that tracks the long-term behavior of gateway nodes and adapts the block validation depending on the reputation of the current gateway node. The proposed reputation consist in frequent updates from the blockchain layer, where each node’s honesty in block mining, B(Gi), is reported based on direct and indirect evidence, and used to update the node’s reputation score. The reputation module further integrates the data trust mechanism to the block validation process by validating: (1) the observation trust values assigned by the gateway, and (2) the device transactions reported in the block to update the reputation score of the gateway node. External sources of a node’s reputation E x t(Gi), which can be imported from other systems, can also be fed into the node’s reputation score. In summary, the reputation score, Rep(Gi) ∈ [Repmin,Repmax], of node Gi is based on a function g : Rep(Gi) = g [T(Gi),B(Gi),E x t(Gi)] where T(Gi) captures how much other validator nodes trust Gi based on Gi ’s trust value assignment to the observations. The reputation of the gateway node increases if the generated block is validated, and decreases otherwise.

Then, since the gateway nodes are known by the network and have permissions to generate blocks, they do not need to compete for block generation using computationally expensive block mining mechanisms. This paper proposes a lightweight block generation mechanism, where gateways generate blocks in periodic intervals.

Moreover, there is an adaptive block validation mechanism. Depending on the reputation of the block generating node, each validator randomly validates a percentage of the transactions in the block.

In summary the advantages of this system are a simple and fast block generation procedure, the use of blockchain to have untampered data, an adaptive block validation technique and a system of trust for devices and gateways. The last two let the system to counter possible malicious devices or gateways in a simple and fast way.

Instead, in summary the weakness are a use of a private blockchain that no privatize the identity of the gateways, a no really secure technique to protect the data between devices, targets and gateways and no way to scale the structure to more user, because of every data is public and visible in the blockchain, so there isn’t a access control system to separate and privatize the data between more users than one.

In my research I utilized the same scheme of the architecture, so divided in gateways and devices, with same interaction. Then I take the idea to utilize a private blockchain for performance reason and the idea of the trust system for the device case to counter possible malicious devices.

GOAL

The target of my research is to give to the structure presented in the paper “A Trust Architecture for Blockchain in IoT” (1) some feature of scalability and privatization of data in the blockchain, with also the aim to show these new characteristics through an example of possible application building a prototype of the end to end process from device to the user in the case localization case.