The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering and Mathematics (EPSTEM), 2025

Volume 38, Pages 771-790

IConTES 2025: International Conference on Technology, Engineering and Science

B-Smart: A Robust Reputation Based Blockchain Scheme in Wireless Sensor Networks

Farah Khedim
University Centre of Maghnia

Nabila Labraoui
University of Tlemcen

Ado Adamou Abba-Ari
University of Versailles Saint-Quentin-en-Yvelines

Abstract: The importance given to wireless sensor networks (WSNs) has made them an ideal target for many security issues. Internal attacks are one of the most serious and dangerous threats resulting from the physical capture of the sensor nodes by malicious adversaries. The internal attacker will extract the cryptographic data and reprogram the captured nodes in order to misbehave and to harm the network. Since traditional cryptographic mechanisms are ineffective against this kind of attack it is essential to find additional detection solutions. In order to make distinction between legitimate and fraudulent nodes, trust and reputation mechanisms have been suggested to overcome the limitations of cryptographic methods in securing WSNs. In these mechanisms, reputation values are assigned to neighboring nodes in honest or dishonest manner according to the legitimacy of nodes assigning those values. However, manipulating and modifying reputation values by malicious nodes make these mechanisms vulnerable to many attacks such as: badmouthing, ballo-stufing, on-off, etc. In this paper, we propose a smart reputation mechanism for WSNs (B-Smart) based on blockchain and smart contracts. The purpose of our protocol is to automate the assignment process of reputation values through the use of smarts contracts to prevent falsification of these values by malicious nodes. Saving these contracts in a blockchain will ensure their durability, integrity and effectiveness. The various evaluations conducted demonstrate the robustness of our protocol against a wide range of internal attacks.

Keywords: Trust and reputation systems, Security, WSN, Blockchain, Smart contract

Introduction

Since their first uses in the military and heavy industrial applications, wireless sensor networks (WSNs) had significant progress and rapid expansion. Self-sufficiency, scalability, responsiveness, reliability and mobility are some of the exceptional characteristics that have made them one of the most innovative multidisciplinary research areas these last years. The recent advent of the Internet of things (IoT) also allowed these networks to become increasingly popular. However, as with almost all technologies, the benefits offered by WSNs are accompanied by significant risk factors and a high potential for abuse (Oztoprak et al., 2024). Indeed, the hostile and unguarded environment in which sensor networks are deployed makes the physical capture of sensor nodes easy for intruders. On the other hand, the limited resources of sensors—such as memory, energy, computational capacity, and communication bandwidth-make the design and development of an effective security protocol particularly challenging (Yilmaz & Dener, 2024).

One of the most serious and dangerous threats to sensor networks is the so-called "node compromise attack". In this attack, the intruder captures a sensor node and extracts all the security and network information. Holding

this information, the attacker injects this data into malicious nodes and reintroduces them among the legitimate nodes of the network. Bypassing security systems and password encryption thanks to their valid cryptographic data, malicious nodes will harm legitimate nodes, delete, modify, and alter the data flow, disrupting the overall functioning of the network. The "node compromise attack" in considered as the entry point of all internal attacks. As cryptographic methods alone cannot counter internal attacks, complementary techniques must be employed to reinforce detection mechanisms and safeguard the sensor network.

Trust and reputation systems (TRS) are proposed as complementary to cryptographic techniques, fostering reliable collaboration among sensors in WSNs (Navaei Tourani et al., 2025). They have been suggested as a powerful tool to distinguish between legitimate and fraudulent nodes, allowing also the identification of malicious, selfish and compromised nodes which have been authenticated (Gupta, 2025) (Moeinaddini et al., 2025). Inspired by human behavior, trust and reputation mechanisms have been able to demonstrate their effectiveness in sensor networks by improving their security, facilitating decision-making and promoting collaboration between nodes (Alzaid et al., 2013). TRS are therefore an effective tool for the detection of "node compromise attack".

Although distinct in definition, the concepts of trust and reputation are closely interrelated and exhibit several common characteristics. Trust, in general, is the degree of confidence with which a node evaluates that another node, or a group of nodes, will execute a given action reliably. (Bhuiyan, 2013; Rodrigues & John, 2020). Using trust assessment provides several interesting properties for sensor networks. It motivates network nodes to behave correctly, since all their actions are monitored and evaluated. It also helps predict future node behavior, which makes it possible to select the safest paths for routing transactions. Finally, it enables the detection of malicious or dishonest nodes (Tenhundfeld et al., 2022). Reputation as it is defined is the cumulative sum of past activities of a node that determines its state of worthiness (Zhang, 2025). The reputation mechanisms provide an incentive for honest behavior and deter dishonest nodes from participating in the network (Pourtahmasbi & Nojoumian, 2022). There is no doubt that conjunction of these two notions provides considerable support for the field of security in WSNs. Enabling the establishment of trust relationships between nodes, evaluation of node reputation and trust management (Zhang et al., 2014).

The adoption of trust and reputation mechanisms in WSNs faces several challenges. First, the large number of nodes, together with limited communication resulting from instability and mobility, makes mutual familiarization and the assignment of reputation values highly complex. Second, the open, unsupervised, and insecure deployment environment, combined with the absence of centralized authority, undermines cooperation among nodes. Collectively, these factors reduce the effectiveness of trust and reputation mechanisms and give rise to significant security vulnerabilities. These security issues result in most cases from the abusive manipulation of reputation values by malicious nodes. The malicious nodes participating in reputation system will thus reduce the reputation values of legitimate nodes in order to damage their reputation and remove them from the network. These nodes will also increase the reputation values of other malicious nodes to increase their chance to participate in critical network functions. The presence of these malicious nodes in the network will thus generate several trust and reputation attacks such as bad mouthing attack, ballot-stuffing attack, on-off attack and conflicting behavior attack.

In this light, the importance of trust and reputation mechanisms in WSNs has been acknowledged by the research community. Considerable research has been done on modeling and creating functional and lightweight protocols. Most of the trust models previously proposed are based on reputation evaluation that by definition is defined as the cumulative evaluation of past behavior of nodes over a certain time interval; this reputation will allow nodes to build trust values (Labraoui et al., 2016). Several methods were used to calculate reputation values based on the number of instances of good and bad behavior. Thus, the success of a reputation mechanism depends entirely on the accuracy with which calculated reputation values predict the quality of future interactions (Sun et al., 2006). Yet, to the best of our knowledge, all the trust and reputation mechanisms presented so far allow any network node to assign and manipulate these valuable values on which the security of the entire network depends. In WSNs, known to be vulnerable to the node compromise attack, at each moment one or more malicious nodes can be introduced undetectably among the legitimate nodes, letting these malicious nodes manipulate reputations values seem incomprehensible and really dangerous. One solution would be to remove the power of attribution of the reputation’s values to the nodes of the network to make a trust model more robust and resistant to the trust and reputation attacks.

In the last years blockchain has emerged as a revolutionary technology that can change the world. "Open source", decentralized, tamper-proof and based on P2P exchanges, the blockchain works without a central authority or trusted third party (Di Pierro, 2017). Smart contracts, which is considered as the blockchain element

with the greatest application potential, offers additional revolution to the blockchain by allowing to automatically be executing predefined conditions in an efficient way and at a high speed. Such characteristics open up many possibilities for sensor networks and broadly benefit the trust and reputation systems.

In this paper, we propose a robust reputation based blockchain scheme in WSNs named B-Smart. The proposed scheme is based on two evolutionary concepts: blockchain and smart contracts. These two concepts will automate the reputation process while ensuring data integrity, availability and security while respecting the specific needs of sensor networks. The main contributions of this work are as follows. Firstly, we introduce the "smart contracts" for the calculation of reputations values. The use of these contracts in our protocol will allow answering most of the problems related to the assignment of reputations values in sensor networks as well as having a mechanism resistant to possible modifications emanating from malicious nodes. Secondly, in order to ensure durability, integrity and effectiveness of all recorded data, our protocol applied the blockchain principle. In fact, the blockchain in our protocol will allow the backup of all the transactions carried out by the nodes in addition to allowing the safeguarding of the smart contract. Allow each node of the network to have a copy of the blockchain will validate transactions, make impossible changes in history and detect any intentional or software malfunction of sensor nodes.

The rest of this paper is organized as follows. Section 2 reviews some related work on trust and reputation mechanisms. In section 3, we describe the background of our protocol. Section 4 described the system model. In section 5, we describe our proposed B-Smart. The main steps of the proposed B-Smart protocol are presented in section 6. Attacks and security analysis are given in section 7. The simulation results are given in section 8. In section 9, we conclude our work and give some prospects.

Related Work

In recent years, we have witnessed an ongoing in the field of trust and reputation systems. Such enthusiasm has given rise to a large number of increasingly innovative and effective protocols. Indeed, as an integral part of our lives, trust has always had a preponderant place for building strong relationships in our daily lives. The application of trust in computer and telecom networks is precisely based on such inspiration. Used effectively in sensor networks, TRS have facilitated decision making by enabling nodes to make appropriate decisions to identify malicious nodes. However, TRSs are victims of their success, and many attackers used them to launch a variety of attacks. These attacks are: bad mouthing, ballot stuffing, on/off, conflicting behavior, whitewashing and intelligent behavior.

A number of protocols have been proposed to mitigate badmouthing and ballot-stuffing attacks, collectively known as dishonest recommendation attacks. During such attacks, the adversary distorts the reputation system by assigning unfairly low (false-negative) values to target nodes in bad-mouthing attacks, or by assigning unfairly high (false-positive) values in ballot-stuffing attacks. The devoted schemes either prevent the occurrence of such attacks or detect these ones once they are present in the network (Khedim et al., 2015).

Prevention based techniques (Khedim et al., 2015). Proposals in this category use one of these two methods: (a) first hand information or (b) positive/negative reputations. In first hand based schemes, the TRS only uses the direct information to calculate the confidence value of the nodes, thus depriving itself of the indirect and yet useful information provided by the neighboring nodes in order to avoid the occurrence of the dishonest recommendations attacks. Although using second hand information, the schemes based on positive/negative reputation only allow propagating of positive or negative reputation values depending on the attack. (Michiardi & Molva, 2002) proposed one of the first reputation protocols. Dedicated to the badmouthing attack, the CORE protocol requires that each node monitors the behavior of its neighbor nodes. A reputation table is used to record these direct confidence values. Using only positive reputation values enable the CORE protocol to counter the badmouting attack. (Ganeriwal et al., 2008) proposed the RFSN protocol for the high-integrity sensor networks. RFSN uses only positive reputation values and higher weight is assigned to secondhand information from a well-reputed node to prevent ballot stuffing attack. CONFIDANT proposed by (Buchegger & Le Boudec, 2002) is one of the best-known reputation protocols. Initialized with positive trust ratings, the nodes continuously monitor the behavior of their neighbors of the next jump. Devoted to the ballot stuffing attack, this protocol only uses negatives reputation values to prevent attackers from increasing the reputation values of other malicious nodes.

Detection based techniques. Instead of simply preventing dishonest recommendations attacks, protocols in this category use complementary methods to detect such attacks once they are in the network. In the Recomm

Verifier protocol (Chen et al., 2012) the reputation management scenario is modeled as a court and the concept of trial is used to strengthen the resistance of the protocol against the dishonest recommendations attacks. For this purpose, a deviation module using an outlier's detection algorithm is applied to filter dishonest recommendations. Then, a temporal verification module makes it possible to recheck the obtained results during the deviation to reduce false positive rate. In Zouridaki et al. (2009), a robust and cooperative confidence-building scheme E-HERMES is proposed. To overcome the problem of dishonest recommendations, the RC test is applied between the first hand information and the second hand obtained information in order to ensure that only recommendations whose value is sufficiently close to the first-hand confidence are accepted. In (Khedim et al., 2018) a bio inspired trust model for mobile WSNs named BTS is proposed. The effectiveness of the protocol is due to the innovative side of the approach. Indeed, by combining between the foraging behavior of the honey bee swarm and two innovative concepts: a modified cloud model and a cognitive chronometry parameter, the BTS protocol allows among others to improve the detection of dishonest recommendations rate and decrease the false positive rate.

Other protocols have been interested on the On/off attack. In this attack, the intruder behaves well and badly alternatively hoping to remain undetectable while causing damage. (Labraoui et al., 2015) proposed the O^2Trust protocol to mitigate the on/off attack in WSN. For this purpose, a penalty policy based on misbehavior history is applied to deal with the dynamic and contradictory misbehavior of malicious nodes. The frequency misbehavior history is then used as a reliable factor when calculating trust values, allowing punishment of malicious nodes. (Chen, 2012) proposed the RASN protocol to resist on/off attack. RASN is built on Trust-Holding-Agent (THA) architecture allowing it to calculate, aggregate and conserve reputation information of nodes. RASN applied two concepts: Latest times of trust mutation and Revision Factor. While, the first concept allows to record the times of trust mutation, the second one allow to deal with all kinds of reputation and to obtain the final trust value. (Amol & Chatur, 2016) present a new efficient and flexible trust management scheme to detect and defend against On/off attack. The protocol relies on two key concepts: Predictability trust and dynamic sliding windows. Predictability allows detecting the on/off attack using sliding windows to keep track of previous behaviors and determine confidence recovery time.

To the best of our knowledge, we have not found any work dedicated on dealing with the conflicting bahavior attack or the intelligent bahavior attack or even whitewashing attacks in wireless sensor networks. In these attacks, the malicious node can create conflict, use intelligent behavior to deceive the TRS and re-enters the system with a new identity and a fresh reputation in unpunished manner. These attacks are at least as dangerous as the previously discussed ones, yet they are often overlooked by trust and reputation protocols, thereby exposing the network to severe damage.

Unlike the existing schemes, our B-Smart protocol allows improving the resistance of the trust and reputation mechanisms against all the aforementioned trust and reputation attacks in addition to being resistant against routing attacks. A reinforced detection method to counter as much as possible the "node compromise" attack known to encompass all the malicious behaviors generated by internal nodes of the network. This is possible thanks to the joint action of several approaches: (1) the automation of the reputation assignment process. (2) The use of a recidivism factor in order to severely punish the malicious nodes and (3) the use of a test period in order to prevent attackers from reentering the system as they please.

Background

Our protocol is the result of the joint action of two main domains (Figure 1): blockchain and smart contract. A brief description of each of these two axes is given in what follows:

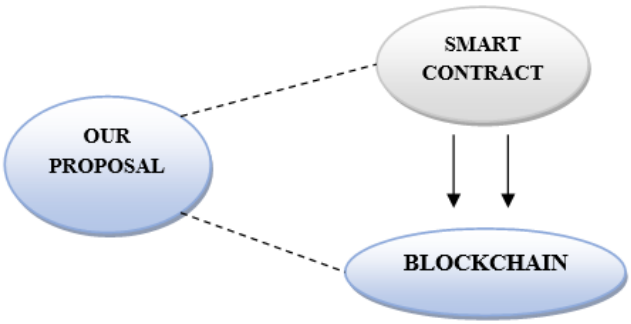

Figure 1. Components of the B-Smart protocol

Blockchain

Blockchain, widely recognized as one of the most transformative technological innovations of recent years, has emerged as a paradigm-shifting technology that has attracted considerable interest across diverse sectors. It enables applications that traditionally required a trusted intermediary to function autonomously in a decentralized manner, without reliance on a central authority. Conceptually, blockchain is a distributed ledger composed of a chain of blocks, recording the history of payments, transactions, and contracts executed and shared among participating entities. To mitigate the risk of a single point of failure (Saleh et al., 2020), the ledger is replicated and synchronized across network members. While blockchain is often associated with Bitcoin, the digital currency introduced in 2008 (Nakamoto, 2008), it can also operate independently of cryptocurrencies.

Three Fundamental Criteria Distinguish Blockchain Technology

Decentralized Architecture

The decentralized side of the blockchain acts as a structural defense against the risk of voluntary changes or data theft from malicious entities. Indeed, the fact that the blockchain is not registered by a single server but by a part of the entities makes the destruction, alteration and modification of data an impossible task.

Cryptographic Protection

Several cryptographic methods are used to secure the blockchain:

- Encryption: The exchanges in the blockchain are secured thanks to the use of asymmetric encryption. The transactions are thus encrypted using the private key of the issuer and can only be decrypted by the corresponding public key. The application of encryption will thus make it possible to guarantee confidentiality, integrity, authentication and non-repudiation in the data network.
- Hashs: The blockchain consists of a set of blocks where transactions are recorded in an orderly and time-stamped manner. Each block consists of two parts: a header and a part dedicated to the recording of transactions. In order to guarantee the integrity of the blocks and to ensure that once a block is validated it can never be modified, the blockchain uses the hash functions. As a result, functions such as the SHA-256 that is currently used in bitcoin and ether are applied. These hash functions are used to calculate the "hash" of a block and insert this value in the header of the next block, to create links between the blocks. Any modification of the data in a block will result in the change of the value of the hash which will thus become totally different from the value of the registered header.

Cryptocurrency Issuance

Inadvertently confused, crypto-currencies are different from the blockchain; however, the two notions are closely related. Serving as a platform, the blockchain makes it possible to record different exchange transactions of these crypto-currencies. Among the crypto-currencies that have emerged: Bitcoin, Ether, Litecoin and Bitcoin cash.

Smart Contracts

Developed in 1994 by Nick Szabo (Szabo, 2017), smart contracts have only become popular for a few years thanks to the meteoric rise of blockchain technology. In fact, based on the blockchain, smart contracts have made it possible to automate and revolutionize traditional contracts by making them unfalsifiable and sustainable.

Running on an Etherum blockchain, Smart Contracts can store data, record information, made decisions and execute contract terms automatically. They can serve as an agreement between entities and the blockchain without the requirement that both parties trust each other (Bagchi, 2017). In addition to these multiple features, smart contracts also benefit from the security side offered by the blockchain. Leveraging these benefits to solve problems related to trust mechanisms and reputation is the fundamental principle of our B-Smart protocol.

System Model

In this section, we describe the network and the threat model. Moreover, we describe the used assumptions.

Network Model

In this paper, we use a WSN network based on blockchain technology. The topology of the network can be indifferently static or mobile. The network follows flat architecture, and the identity of each node is unique and stable.

Threat Model

In this paper, we assume an active attacker model in which a malicious node voluntarily tries to remove, alter, modify, misroute or replay the messages transmitted on the network that it is supposed to forward under a given routing protocol. Such an attacker with "bad behavior" tries to cause maximum damage and disrupt the functioning of the network. Conversely, a node that propagates messages correctly is defined as having "good behavior".

Assumptions

Any trust and reputation management scheme must initialize the trust and reputation values before the deployment of the network. Therefore, in our protocol B-Smart we assume that: 1) the reputation values belong to [0, 1]. 0 means very bad behavior and 1 means very good behavior. 2) At the beginning of the lifetime of our network all the nodes have an equally good reputation equal to 0.5 and are equally trusted. The reason is simple: at the very beginning of the deployment, no malicious opponent has had the time or the chance to influence or subvert a node. 3) New nodes appearing during network lifetime should not be fully trusted, as they could be generated by an adversary. These nodes are placed in a *"test period"*; they must perform a greater number of satisfactory tasks compared to the initial nodes before they can recover a normal reputation value.

Vocabulary

In the following, we described the following notations and expressions considered in our protocol. (Table 1) gives the considered notations.

Table 1. Notations

Notation	Description
TRS	Trust and Reputation System
TR_X	Transaction x
S	Source node
D	Destination node
SK_i	Private key of node i
PK_D	D's public key
$Sig_{SKi}(TR_x, PK_D)$	Signature on TR_X by node i
Rec_i	Recidivism factor for node i
Rep_i^{last}	Last assigned reputation to node i

B-Smart Protocol

The panoply of trust and reputation protocols proposed in recent years has proved the effectiveness of TRS for the detection of a large number of attacks. They have become an essential tool for solving security problems in wireless sensor networks. However, their effectiveness is destroyed in the face of internal attackers. These malicious nodes try to deflect the trust and reputation system by manipulating the reputation values of neighboring nodes as they please and communicate these distorted values to the other nodes of the network.

In this section, we propose a smart reputation mechanism for WSNs (B-Smart) based on blockchain and smart contracts. The main objective of the B-Smart is to automate the assignment process of reputation values through the use of smarts contracts to prevent falsification of these values by malicious nodes. Saving these contracts in a blockchain will ensure their durability, integrity and effectiveness. We present in the following the design goals of our protocol B-Smart, the system architecture as well as the main phases of execution.

Design Goals

Our reputation protocol based on blockchain and smart contracts aims to meet several security objectives, namely, decentralization, information integrity, availability of reputation values and non-repudiation:

- Decentralizing. B-Smart allows a backup of all transactions in a decentralized manner in all nodes of the network without relying on a third party thanks to the use of a blockchain topology.
- Centralization of calculating reputation values. Removing power from sensor nodes to assign reputation values to other network nodes helps to prevent an attacker from using the mechanism to manipulate reputation values as needed by decreasing legitimate reputation values or increasing those of the other attackers. Entrusting the calculation of reputation values to a central entity "smart contract" and save it in the blockchain not only facilitates access to them but also ensures decentralization and security, thus avoiding the traditional disadvantages of centralized methods.
- Information integrity. B-Smart allows keeping track of all the transactions made in an unchangeable way. The use of the blockchain ensures that the information stored in the blocks cannot be changed by any node of the network.
- Reputation values availability. The use of the smart contract makes it possible to guarantee the availability of the reputation values for the different nodes of the network. Indeed, any node can know the reputation values of its neighbor nodes without having to ask from recommenders.
- Non-repudiation in the B-Smart protocol is ensured through the use of asymmetric cryptography. Indeed, tracking the routing of the transaction through the different intermediate nodes will prove that a message was sent by its sender or received by the recipient.

General Description

B-Smart is a novel reputation based blockchain scheme. The proposed protocol overcomes the problem of the malicious manipulation of reputation values by entrusting the management of these values to a smart contract. This smart contract will thus follow the progress of the various transactions of the network and assign to the nodes the corresponding reputation values according to their behavior. The nodes will thus be judged according to whether they send the messages correctly or not, the presence or absence of modifications in message packets, a change in the routing path of the packet as well as on the possible deletions of the messages in transit. A *recidivism factor* is applied by the smart contract when calculating reputation values in order to severely penalize malicious nodes by significantly reducing their reputation values. This factor also helps motivating the intermediate nodes to relay the information correctly in order to preserve their reputation values. Automating the reputation calculation process not only overcomes the problems associated with the manipulation of reputation values by malicious nodes but also allows us to avoid selfish nodes and offers an efficient solution to isolate malicious network nodes. The smart contract is saved in the blockchain to ensure its durability, integrity and effectiveness. Thus recorded, the contact is protected from abusive manipulation by internal attackers.

The B-Smart protocol works as follows: when a node wants to send a message or to request information from another node or from the base station, this communication follows the following main steps: Firstly, a routing protocol is used to determine the optimal path between the requester and the provider. Indeed, the message or request must pass through several nodes in a "multi-hop" mode since "one-hop" communications are resource-intensive in WSNs. Secondly, time is allocated for each transaction, and a block is created to track the routing of the transaction between each successive nodes to its destination or until the time is over. Once the transaction is completed or its time is over, the block is inserted into the blockchain. A personal copy of the blockchain is hosted by each node to guarantee its security. However, given the limited storage capacity of the sensors, we assume that the nodes can store it in any kind of network accessible storage, privately hosted, such as the cloud or decentralized storage such as Swarm (Hartman et al., 1999) or IPFS (Benet, 2014) or other types of storage (Bagchi, 2017). Finally, the smart contract uses the data contained in its history as well as the information provided by the block of the transaction in order to update the reputation values of the participating nodes. Nodes with reputation values below a defined threshold are declared as malicious and embedded in the blacklist

to prevent their participation in network applications. The Overview of the B-Smart protocol is given in (Figure 2).

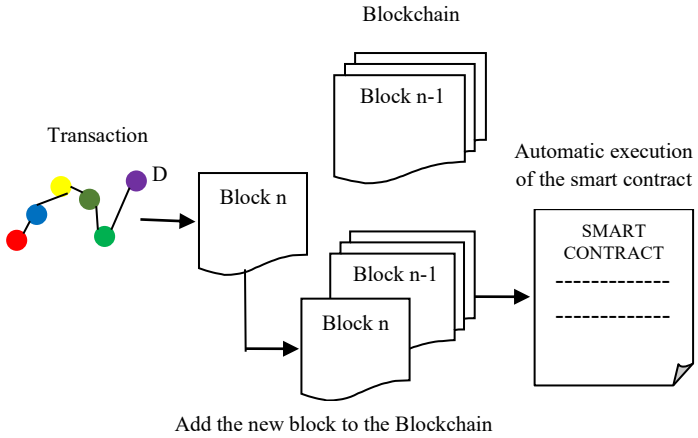

Figure 2. Overview of the B-Smart protocol

System Architecture

The B-Smart protocol is based on the joint operation of several entities. Among these entities, we can mention:

Transaction

The interactions between the sensors are the fundamental principle of any sensor network. Indeed, the exchange of information such as temperature, humidity and other parameters between these nodes will allow the implementation of various applications. A transaction is therefore any data exchange between the nodes, as well as between the nodes and the base station. Each transaction in our protocol involves a source node (S), a destination node (D) and a number of intermediate nodes for relaying it. Node (D) plays the role of requester, and node (S) plays the role of provider. Transactions in our protocol are stored in blocks using a blockchain data structure. Each transaction is cryptographically signed by all participants in order to keep irrefutable proof of the participation of each user involved in the transaction.

Node

In our protocol a sensor node can play the role of provider, requester or gateway node. As the requestor, the node will request the recovery of some data from the provider node. The provider is responsible for transmitting certain files, messages, or the sensed data to the requestor with the help of the intermediate nodes. The latter, will create a block that will track the routing of the transaction in a peer-to-peer manner through the multi-hop gateway nodes to the requesting node. Each node participating in a transaction in our protocol must have a unique signature; this signature is formed by a pair of public key and private key. While the public key is shared with all the nodes of the network, the private key remains secret. Elliptic Curve Cryptography (ECC) is applied to generate public key from private key thus offering a great degree of security while being adapted for sensor networks thanks to the reduced size of the keys compared to other cryptographic methods such as RSA (Yan, 2022).

Block and Blockchain

A block is used to save all the information relating to the routing of the transaction from a source node to a destination node. Indeed, all the actions of the nodes during a transaction are recorded in the block, such as: the sending, the reception, the modification as well as the deletion of data. In our protocol, each block contains one transaction. The statement of the transaction and the different steps of the routing of the transaction with their corresponding time stamps are defined in the body of the block. To link the blocks together and thus guarantee the integrity of the blocks, the hash function SHA-256 is used to calculate the "hash" of a block and insert this

value in the next block header. Any modification of the data in a block will result in the change of the value of the hash which will thus become totally different from the value of the registered header.

Smart Contracts

A smart contract is a special block that will perform the reputation protocol. It is automatically executed after adding a new block in the blockchain. Using the information contained in the block concerning the routing of the transaction by the sensor nodes and using his personal history, the smart contract will be able to judge the nodes, to assign the appropriate reputations values and to update the existing reputation values. Accessible via a contract address, the nodes of the network can communicate with the smart contract by sending messages to its address. These messages can be either *Transaction* or *Call.* Transaction messages are sent when the nodes require storing pertinent information of specific devices. Call messages are made when nodes want to query the state of a device at a given time (Bagchi, 2017).

B-Smart Scheme

To explain how our protocol works, we assume that the transaction happens between two nodes, i.e., node source S and node destination D in a multi-hop manner. The whole steps performed in the execution of the B-Smart protocol are highlighted in (Figure 3) and explained in the following:

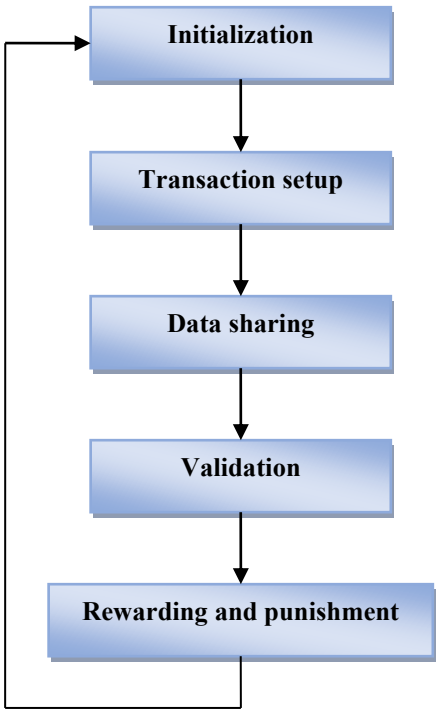

Figure 3. The main steps of the proposed B-Smart protocol

Initialization Phase

A routing protocol is applied to determine the most appropriate path between the source and destination node. Several routing protocols allowing the discovery of the optimal path have been applied efficiently in the sensor networks. These protocols consider several parameters such as: the energy level of the sensors, the reliability on data delivery, the number of hops and the security of the path. In our protocol these factors are only taken into account during the first rounds. Once the smart contract has more knowledge about the reputation of the nodes, the routing protocol will refer to the information provided by the smart contract to choose the safest way. The existing routing protocols are classified into three main categories (Othmen et al., 2016): reactive, proactive and hybrid routing protocols. In reactive protocols such as (AODV) (Perkins, 2003) and DSR (Johnson & Maltz, 1996), the node discovers a path with the destination on demand. This is done by flooding the network with

Route REQuest packets (RREQ). This can lead to a high latency time in the route-finding process. In proactive routing protocols such as DSDV (Perkins & Bhagwat, 1994) and OLSR (Clausen & Jacquet, 2003), each node maintains fresh lists of destinations and their paths by periodically distributing control messages. This solution is suitable when the topology is static. However, it has slow reactions on restructuring and failures. Whereas hybrid protocols such as ZRP (Haas & Pearlman, 2000) and ZHLS (Hamma et al., 2006) combine the advantages of the reactive and proactive protocols. Choosing a routing protocol instead of another is out of scope this paper since it will depend on the needs of the application.

Transaction Encryption

Once the routing path is established, the requesting node concretizes its intention to initiate a transaction by creating a corresponding block. The head of the created block contains the statement of the transaction and the path defined by the routing protocol. The body of the block will follow and record all the steps of routing the transaction between the intermediate nodes to the destination. Encryption of the transaction is realized thanks to the use of asymmetric encryption and more particularly elliptic curve cryptography (ECC). The use of asymmetric cryptography will ensure the authentication and integrity of the data relayed through the gateway nodes. Since each node of the network has a pair of keys (public key and private key), the provider node S will use the public key of the requester node D (PK_D) to encrypt the message that its wants to send him conveyed by the transaction TR_x. Each gateway node G_i must in turn sign the data in transit in order to keep track of the routing of the transaction. (Figure 4) describes the main steps of the transaction encryption.

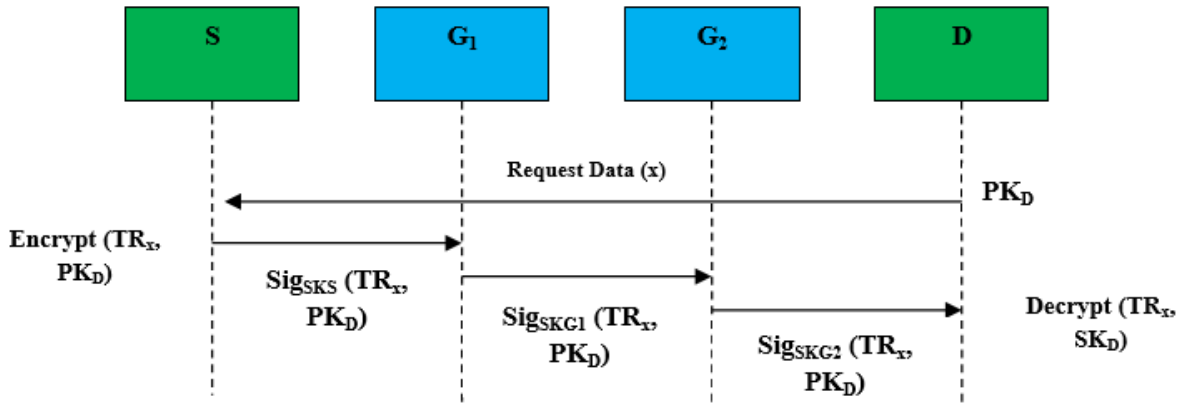

Figure 4. Main steps of transaction encryption process

Data Sharing

The encrypted transaction is sent in multi-hop manner from the source node to the destination node. Any changes and alterations, as well as each successful reception and sending by the gateway nodes, are recorded in the transaction block maintained by all the nodes participating in the transaction.

Transaction Time

A defined time is allocated to each transaction. At the end of this time the transaction is considered complete. This time, will limit the time spent on transactions in order to overcome the problem of transactions that never reach their destination due to hardware failures or voluntary deletions by malicious nodes, thus avoiding waiting indefinitely.

Block Validation

Unlike existing blockchain like those in (Underwood, 2016; Madisetti, 2016) where block validation is performed by a set of miners to validate the block before integrating it into the global blockchain, in our protocol, the validation is carried out by the smart contract once the block is integrated in the blockchain for two main reasons. On the one hand, the use of miners implies a significant consumption of computation power of the latter, in the WSNs known for their limited resources; such calculations will significantly reduce the energy of

the miner's sensors which will reduce the duration of the network lifetime. On the other hand, in a traditional blockchain, the miners will check the transactions to prevent fraudulent operations; those considered invalid will never be integrated in the blockchain. In B-Smart, integration into the blockchain of all transactions will allow us to detect and to prove the offense of malicious nodes by having an irreversible proof of their fraudulent behavior in the routing of transactions. During validation, the smart contract will check the consistency of the transaction. It will then verify that the transaction has followed the path indicated by the routing mechanism; the signatures and the consistency of the transactions. The results of this analysis will be taken into account in the next step.

Rewarding and Punishment Phase

After the validation step, the smart contract has enough elements to judge the behavior of the different nodes of the transaction and to assign them the corresponding reputation values. The simplified architecture of the smart contract is shown in (Figure 5) and the corresponding algorithm is given in Algorithm 1. More specifically, once a bloc is added to the blockchain, the smart contract is applied in automatic manner to verify that the terms of the contract have been respected, in our case this states that the transaction has been carried out correctly. The smart contract holds a reputation table of all the nodes of the network. The values of the nodes that participated in the last transaction are updated after each new transaction.

The reputation table is composed of three columns. The first column, *Node (Ni)*, contains the identities of all nodes in the network. The second column, *Recidivism factor (Reci)*, records the number of times a node has misbehaved. The higher this counter, the more critically the reputation value of the malicious node decreases. Finally, the third column, *Last reputation value (Repi_last)*, stores the most recent reputation value assigned to the node by the smart contract. The table is easy to maintain. For example, in a transaction when the evaluated node or a gateway node transfers a packet for the next node correctly "good behavior" then its Rec_i is unchanged and its reputation value Rep_i^{last} is increased by a value α. Without lost of generality, we took α=0.05. Otherwise, if one of the gateway nodes drops the packet or modifies it before the transfer for malicious or authentication reasons "bad behavior", then its Rec_i is increased by one and its reputation value is divided by the exponential of the value (Rec_i). This last operation resulted in a critical reduction of the reputation value of the malicious node. The process of assigning reputation values by the smart contract, although simple, can severely punish the malicious nodes by making reputation difficult to acquire but easy to lose. This will help to deter malicious nodes from disrupting network operations and provide our protocol with an effective method of detecting and isolating them. This process also allows the intermediary nodes to relay the information correctly. Nodes with a reputation value below a defined threshold are declared malicious and blacklisted to prevent their participation in network applications.

Algorithme 1. The attribution of reputation values process

Begin

1. **For each** Transaction_sensor (i)
2. **if** Good_Behavior (i) **then**
3. $Rec_i = Rec_i$
4. $Rep_i^{last} = Rep_i^{last} + \alpha$
5. **else**
6. $Rec_i = Re_c^{i+1}$
7. $Rep_i^{last} = Rep_i^{last} / \exp(Rec_i)$

End

Automating the assignment of reputation values by smart contract allows our protocol B-smart to create trusted transactions without central control and without the intervention of sensor nodes while maintaining integrity, confidentiality and resistance to a large number of internal attacks. In summary, in order to have a clear view about the operation of our proposed scheme, we provides in (Figure 5) a flowchart showing the various phases and the whole operations of the B-Smart protocol.

Attacks and Security Analysis

While effective, trust and reputation mechanisms may be victims to a large number of attacks that we will commonly call "trust and reputation attacks". These attacks have tarnished the usefulness of these mechanisms

and discouraged their use especially in sensor networks. Indeed, suffering from a great lack of security, sensor networks are already vulnerable to a large number of internal attacks; the use of trust and reputation systems adds an additional security problem. Our protocol B-Smart protocol helps to fight the trust and reputation attacks, a way for us to improve the image of trust and reputation systems so that they can act effectively to secure sensor networks. We will present in the following the main attacks that threaten these mechanisms as defined in (Yu el al., 2012), as well as the strategies used by our protocols to detect and eliminate such attacks.

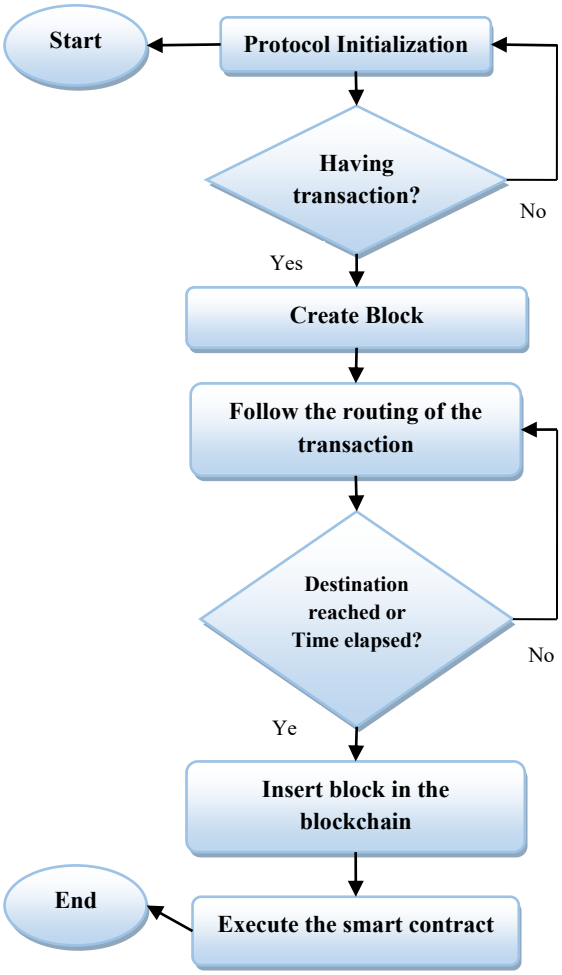

Figure 5. Flow chart of the B-Smart protocol

Trust and Reputation Attacks

This category includes all attacks that use the trust and reputation mechanism to perform malicious actions. These attacks are as follows:

Bad Mouthing Attack

Trust and reputation mechanisms often use recommender nodes to obtain information on certain nodes of the network. The recommender nodes thus make it possible to provide second hand information that is very useful for the evaluating node in order to complete its vision on a node that it knows little or that it doesn't know. In the case where the recommenders are honest; this indirect information greatly enhances the effectiveness of trust and reputation mechanisms. However, malicious nodes can be introduced among these recommenders as is the case in the bad mouthing attack. In this attack, the attacker handles the trust and reputation system to assign unfairly negative values to legitimate network nodes. This attack leads to deform the reputation of the nodes and thus to distort the results of the confidence system. One of the main consequences of such an attack is the isolation of legitimate nodes from critical network applications due to their reduced reputation values, thereby allowing malicious nodes to occupy more space and ultimately impose themselves as leaders. Although our B-

Smart protocol does not rely on second-hand information, it is just as much, if not more, effective as protocols that rely on this indirect information since the smart contract has a global view of all transactions running in the network. By not involving any recommender in the calculation of reputation values, B-Smart is completely resistant to this type of attack.

Ballot Stuffing Attack

As in the aforementioned attack, the malicious node will be introduced among the recommenders. However, unlike the bad mouthing attack, it will not assign negative values, but false-positive reputation values to another malicious node in the network. The main purpose behind this attack is to favor attacking nodes by increasing their reputation values in order to increase their weight in the network. Automating the assignment of reputation values process thanks to the use of smart contract protects our B-Smart protocol against this type of attacks.

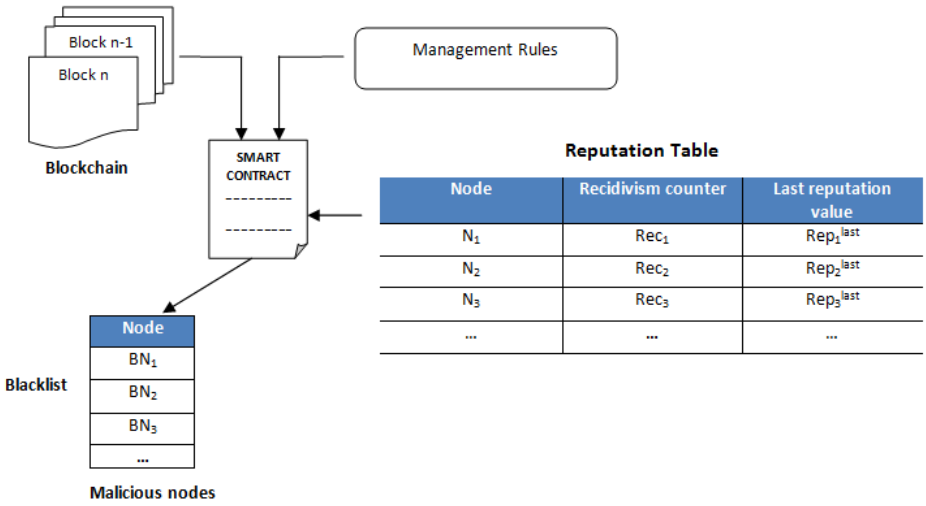

Figure 6. Simplified architecture of smart contract in B-Smart

On/Off Attack

In this type of attack, the malicious node will proceed in two phases, a phase "on" and a phase "off". During the "on" phase, the attacker launches the attack. It will act negatively in the network, taking advantage of its high reputation value which will allow him to remain undetectable for a moment. During the "off" phase, the attacker will behave correctly to increase its reputation and gain the trust of those around him. This attack is efficiently handled in our B-Smart protocol. Indeed, during the phase one, the attacker will have good behavior which will bring him an increase in its reputational value. The smart contract will thus increase its Rep_i^{last} of α (with α= 0.05) as long as Rec_i= 0. During the off-phase, the attacker will behave in a malicious way; its recidivism factor will thus increase by 1 to each bad behavior. The process used in the calculation of reputation values by the smart contract allows for a small increase in reputation values in the case of good behaviors but leads to an exponential decrease of these values during malicious one. So, even if the malicious node generating an on / off attack can increase its reputation value, this value will drop below the threshold of honesty (β= 0,3) after only 1 to 2 bad behaviors at the most.

Conflicting Behavior Attack

In this attack, the malicious node behaves differently with the nodes of the network. Indeed, it will have good behavior with a few nodes, which will earn it positive reputation values. On the other hand, it will behave in a prejudicial way with the other nodes which will therefore judge it negatively. The conflicting behavior will occur when the nodes of the first group will exchange on the reputation of this malicious node with the other nodes. Having different reputation values will undermine the trust of the nodes of the first group in relation to those of the second and vice versa, thus creating conflict. The problematic relating to this attack does not arise in our B-Smart protocol. Indeed, the node is judged independently in each transaction. If it has a good behavior its reputation is increased, otherwise the latter will tend to decrease tragically. Therefore, whatever an adversary performs, it has no power to create a conflict.

Intelligent Behavior Attack

In this attack, the malicious node is extremely intelligent. It will indeed adapt its behavior according to its reputation value. As a result, it will behave differently at each time period by selectively providing good or bad services or by assigning low or high recommendation values based on the confidence level. To try to remain undetectable in the network against our B-Smart protocol, the intelligent attacker has no choice; it must absolutely adopt a good behavior in the majority of the cases. Because otherwise, the recidivism factor that we used will quickly decrease its reputation value which will earn it the isolation of the network and integration in the blacklist. By keeping a good behavior, the attacker will not have a negative impact on the network.

Whitewashing Attack

Reputation systems are known to be particularly vulnerable to whitening attacks. In this attack, a malicious node whose reputation value has greatly diminished has the opportunity to re-enter the network with a new identity and a fresh reputation. To parry these attacks, the new nodes in our protocol are not completely trustworthy; they must pass a test period in which they will have to perform a large number of satisfying tasks in order to gain a normal reputation value. This process is similar to the "proof of work" procedure used in blockchain. It allows discouraging this type of attack because by reentering the network with a new identity the attacker must provide a lot of effort and consume a lot of energy resources. In addition to being resistant to reputation attacks, our B-Smart protocol perfectly detects routing attacks. We describe in the following the main routing attacks and the means used by our B-Smart protocol to fight against them.

Routing Attacks

We include in the category of routing attacks all attacks that threaten the routing of information by deleting, altering, modifying or bypassing the transit path of messages.

Spoofed, Altered, Replayed Information

In this type of attacks, malicious nodes aim to fabricate non-existent information, change some data and replay messages to disrupt network operation especially by creating routing loops or increasing end-to-end latency. The detection of this attack in our protocol is done through the comparison made by the smart contract between the information contained in the head of the block (the main statement of the transaction, the routing path defined by the routing protocol) and the various phases of execution of the transaction through the different nodes. Such a comparison allows noticing immediately any change in the body or in the routing of the transaction. B-Smart effectively detects this type of attack and our recidivism factor will severely reduce the reputation values of the compromised node.

Selective Forwarding Attack (Greyhole Attack)

Similar in several points, the selective forwarding and the greyhole attacks both refuse to send messages to certain nodes or to certain destinations. The comparison made by the smart contract between the header of the transaction block containing the routing path defined by the routing protocol and the path followed by the transaction during its execution, allows effective detection of any deviation from the initial path. The B-Smart protocol allows an effective detection of these two types of attacks and can severely punish the nodes responsible for malicious behavior.

Sinkhole, Blackhole and Wormhole Attacks

These three attacks share the fact that they are placed in an optimal routing path in order to capture a maximum of traffic. Data passing through these attackers are recovered and never retransmitted. Indeed, the malicious node will be placed on the road leading to the base station during the sinkhole attack. By manipulating the routing tables, the compromised node will be closer and more attractive than in reality to attract as much data as possible during the blackhole attack. Tricking nodes over distances and influencing the routing tables through the creation of low latency tunnels during the wormhole attack. The development of the routing paths in our

protocol is independent of the nodes. It is indeed carried out thanks to the information provided by the smart contract. So, a node wishing to generate one of these three attacks has no influence on the other nodes to force them to transmit the data through it. In the case where one of the attackers is included in a routing path because it has a high reputation value, its reputation value is downright diminished once it performs its malicious task. It will never be chosen anymore to route information.

Sybil Attack

In this attack, the malicious node illegitimately creates a large number of malicious nodes in order to have a disproportionate influence in the network. Although our protocol fails to detect this type of attack, the *"test period"* applied for the new nodes of the network allows us to prevent this attack and to discourage its occurrence. Since the newcomers must perform a number of satisfying tasks in order to obtain a normal reputation value. On the other hand, the least malicious behavior will be penalized by a significant reduction in reputation value.

Node Replication Attack

In this attack, the attacker creates several replicas of a same node named "clones". These replicas have the same key pair and the same identifier. Since the smart contract holds a table with all node IDs, reputation values, and recidivism counter, the more the malicious node creates malicious replicas, the faster the node recidivism factor will increase, and the reputation value will decrease accordingly. In the extreme case where the node will try to remain undetectable by creating only one replica, our B-Smart protocol will detect this attack just as easily as the recidivism counter will increase twice as much as attacks generated by a single node.

Simulation Results

In this section, we present results of our simulations showing the performance of our reputation model. Two simulation experiments are carried out to validate the effectiveness of our proposed scheme. Firstly, we analyze reputation evaluation process of our B-Smart protocol. Secondly, we check the effectiveness of our scheme by considering the impact of two main attacks: on/off and conflicting behavior. MATLAB software is used as simulation tool to assess the performance of our protocol. A comparison is made between B-Smart, RaRTrust (Labraoui et al., 2015) and RFSN (Ganeriwal et al., 2008) in the On/off attack scenario and between B-Smart and ATSN (Chen et al., 2007) in the conflicting behavior attack scenario.

Simulation is set up as follows. All nodes of the network are initialized with the same reputation value equal to 0.5 and are considered trust. The behavior of the nodes is judged according to all the transactions in which they participate. A recidivism factor Rec_i is assigned to each node of the network. This counter is used to record the number of bad behaviors performed by the node. The reputation value of node i will entirely depend on the value of this counter. The default simulation parameters are summarized in (Table 2).

Table 2. Simulation parameters

Parameter	Default Value
Area (m^2)	100 x 100
Number of nodes	100
Radio Range (m)	25

Reputation Evolution Analysis

Existing TRS are either based on direct information or on both direct and indirect information when calculating confidence values. Both methods have advantages and disadvantages. In fact, using only the first-hand values effectively protects the protocols from malicious recommendations attacks. However, this method has serious drawbacks. Indeed, lot of time is needed to establish the reputation values and these values will also take a lot of time to decrease, allowing the attacker to stay longer in the network. On the other hand using also indirect ones can provide additional information to nodes about other nodes they know little or they do not know. However, they expose themselves to possible presence of malicious nodes among these recommenders.

In this section, we analyze the process of automating the calculation of the reputation values of our B-Smart protocol based on the use of the smart contract. For this purpose, we compare the behavior of our protocol with two trust and reputation protocols based on the use of first-hand and second-hand information namely RFSN (Ganeriwal et al., 2008) and RaRTrust (Labraoui et al., 2015). Direct observation in RaRTrust and in RFSN are called DT-RaRTrust and DT-RFSN respectively and indirect observations are called as IT-RaRTrust and IT-RFSN respectively.

Case (1). The scenario is as follows: we perform an analysis on the evolution of the reputation values of a given node i. This node is a legitimate node of the network, initialized with a reputation value equal to 0.5. It has a good behavior during the first 40 units of time. At some time tps ∈ [40, 50] this node is compromised. At tps = 50, it starts its malicious behavior.

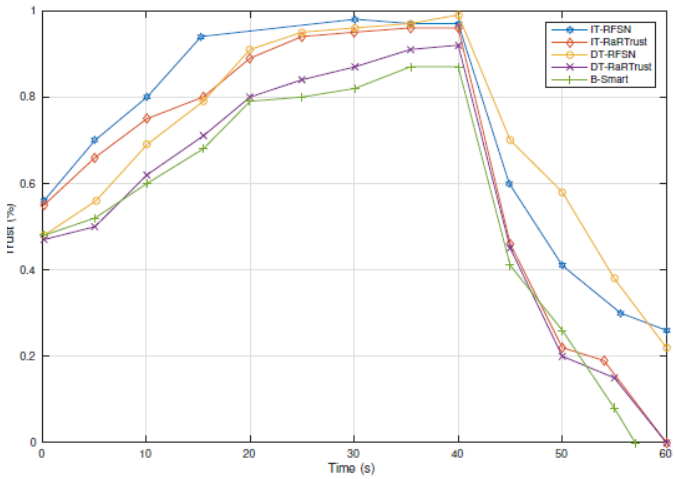

Figure 7. Reputation values evolution.

We can show clearly from (Figure 7) that reputation values of node i increase slowly in our protocol than in other protocols. This can be explained by the fact that the reputation value increases by α at each good behavior of the node, a slow and linear increase encouraging the nodes to have a large number of good behaviors in order to acquire a high reputation value. On the other hand, at the first "bad behavior", the reputation value of the node will plummet faster than in the RFSN and RaRtrust protocols thus allowing for our B-Smart protocol a faster detection of malicious nodes. These results are possible thanks to automation of the reputation calculation process in our B-Smart protocol through the use of an independent, unbiased and secure entity namely "smart contract". This automation allows the network to enjoy the benefits of the first hand and second hand methods while being resistant to their disadvantages.

Trust and Reputation Attacks Analysis

The primary goal of automating the assignment of reputation values process is to strengthen the resistance of the trust and reputation mechanisms against attackers who use them to launch a multitude of attacks such as: bad mouthing, ballotstuffing, on/off, conflicting behavior, intelligent behavior and whitewashing attacks. In this section, we analyze the resistance of our protocol against two main attacks that threaten the TRS namely: on/off and conflicting behavior attacks. Dishonest recommendations attacks including badmouthing, ballot-stuffing and collusion are not taken into consideration in our simulations since our protocol is perfectly resistant to this type of attacks. Indeed, the use of smart contract relieves the nodes of having to ask for reputation values from recommender's nodes.

On/Off Attack Resiliency

During on/off attack, malicious nodes behave well and badly alternately, hoping to stay undetectable while causing as much damage as possible. For instance, in this attack, once the malicious node acquires a high reputation value in the off phase thanks to it good behavior, i.e., forwards messages correctly, it begins the on stage of the attack by acting in a malicious manner i.e. drops, alters or modifies messages. The simulation scenario of this attack is the following:

Case (2). We consider a malicious node i. In the off phase, node i correctly transmits the messages in each transaction where it is involved. It launches the on phase of the attack at tps = 6 units of time. This cycle on is immediately followed by an off cycle at tps = 10.

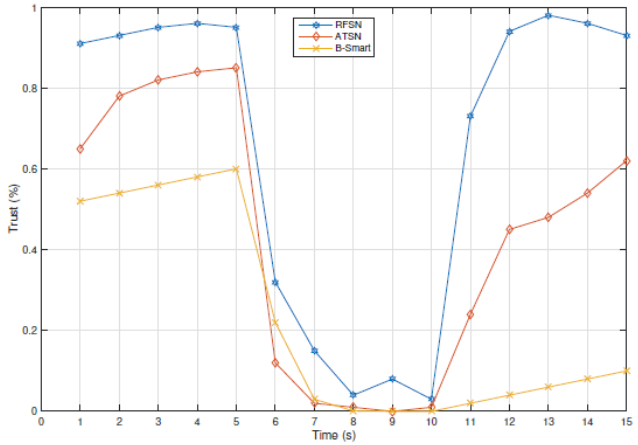

Figure 8. On/off attack of node i.

(Figure 8) shows the simulations comparison results performed between our B-Smart protocol and the ATSN (Chen et al., 2007) and RFSN (Ganeriwal et al., 2008) protocols. In our protocol the reputation value of the malicious node i increases slowly during the off phase of the attack and its corresponding recidivism counter is at 0. During the on phase, the reputation value of the node i decreases sharply in BSmart as the recidivism counter Reci of the node i increases with each bad behavior. This exponential decrease allows a quick and efficient detection of the malicious node. In the RFSN protocol also the reputation value decreases rapidly also, however, the latter increases more rapidly during the off-phase of the attack. Indeed, contrary to the RFSN protocol, B-Smart remembers the malicious behavior of the node since the value of the recidivism factor associated with node i is permanently stored in the smart contract held by the blockchain. So, even if during the next phase off, the malicious node manages to increase its reputation value slightly, it will decrease even more sharply in the next phase "on" given the already high values of the recidivism counter. We can conclude that our B-Smart protocol is more efficient than ATSN and RFSN for the detection of the on/off attack. Its operating principle based on the use of recidivism counter as well as a smart contract allows an increasingly rapid detection of this attack from one cycle to another.

Conflicting Behavior Resiliency

Although insidious, conflicting behavior is an attack that has not achieved much interest from researchers working on the field of security in trust and reputation mechanisms in WSNs. This attack has the power to create conflicts between groups of nodes thus creating a lack of mutual trust between them. At this attack, a malicious node i behaves well with a group of nodes (A, B and C), i.e., correctly sends the messages in transit of these nodes, they will assign him positive reputation values. In parallel, the same malicious node i will behave badly with a second group of nodes (F and G), i.e., delete, alter or modify the messages of these nodes. They will therefore assign him negative reputation values. The conflict occurs when a node in the first group (exp: A) exchanges with a node in the second group (exp: F) on the reputation of that malicious node. Node (A), which is sure that i is a legitimate node, will think that node (F) is lying to it and will judge F as malicious and vice versa.

Case (3). In this scenario, the node i launches a conflicting behaviour attack. It will behave differently with two distinct groups of nodes.

Figure 9 shows the results of the simulations performed during the conflicting behavior attack. We notice that in the ATSN protocol, node (A) continues to communicate with the malicious node i as long as it behaves in a good way with it. Node (A) will continue to trust the node i and give it a good reputation. Unlike node (A), node (F) assigns negative reputation values to node i because of its malicious behavior and stops cooperating with it. The reasoning of the ATSN protocol is not entirely correct for two main reasons: on the one hand, the node i is a malicious node and the fact of continuing to communicate with him exposes the node (A), the nodes of the first group as well as the entire network to various damage. On the other hand, by fully trusting the malicious node i, the nodes of the first group are exposed to a conflict with the nodes of the second group, a lack of confidence that can cause revocations of legitimate nodes deemed injuriously malicious.

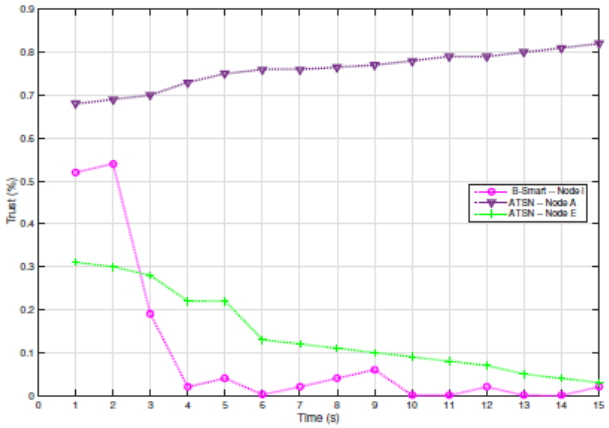

Figure 9. Conflicting behaviour attack of node i.

In our B-Smart protocol, the smart contract is responsible for calculating all reputation values by holding for each node a recidivism counter and a reputation value. These values are updated after each new transaction. This automation and independent computation of the nodes reputations values make it possible to judge impartially the nodes behaviors. The results of the curve of our B-Smart protocol clearly demonstrate this operating spirit. Indeed, as soon as the malicious node misbehaves its reputation value will decrease and conversely when it acts positively. We can conclude that our B-Smart protocol outperforms the ATSN protocol facing the conflicting behavior attack.

Conclusion

The effectiveness of trust and reputation systems in WSNs is no longer to be proven. However, the development of such mechanisms creates additional security issues for these networks. Indeed, malicious nodes introduced into these systems will have the power to manipulate the values as they please, thus distorting the results of the TRSs. We presented in this work a robust reputation based blockchain scheme in WSNs, which is designed to address the problem of abusive manipulation of reputation values by malicious nodes. In our proposal B-Smart, the calculation of reputation values is entrusted to a smart contract; an independent and secure entity, making it possible to judge the behavior of the nodes impartially and assign them the corresponding reputation values. The backup of all transactions as well as the smart contract in a blockchain structure will ensure their durability, integrity as well as resistance to any intentional modification by malicious nodes. Automating the assignment reputation values process thanks to the smart contract offered our protocol a great resistance as well as an effective detection of many internal attacks. Indeed, security analysis demonstrates the resiliency of B-Smart against trust and reputation attacks as well as routing attacks. Besides, our simulation results demonstrate that the proposed scheme can efficiently isolate malicious nodes from the network. The different simulation scenarios proved the effectiveness of our protocol under various attacks scenarios. As a future work, we intend to use our protocol for securing the multi-path routing in WSNs.

Scientific Ethics Declaration

* The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Conflict of Interest

* The authors declare that they have no conflicts of interest

Funding

* This work has no funds

Acknowledgements

* This article was presented as virtual presentation at the International Conference on Technology, Engineering and Science (www.icontes.net) held in Antalya/Türkiye on November 12-15, 2025.

References

Alzaid, H., Alfaraj, M., Ries, S., Jøsang, A., Albabtain, M., & Abuhaimed, A. (2013). Reputation-based trust systems for wireless sensor networks: A comprehensive review. In *IFIP International Conference on Trust Management* (pp. 66-82). Springer.

Amol, R., & Chatur, D. P. (2016). Detection of on-off attack based on predictability trust in wireless sensor network. *International Journal of Advanced Computational Engineering and Networking, 4*(12).

Bagchi, R. (2017). Using blockchain technology and smart contracts for access management in IoT devices. *Computer Science, 80*(9). https://helda.helsinki.fi/server/api/core/bitstreams/97b74ad0-c46c-41ea-a42b-5f967370a64b/content

Benet, J. (2014). IPFS-content addressed, versioned, P2P file system. *arXiv*.

Bhuiyan, T. (2013). *Trust for intelligent recommendation*. Springer.

Buchegger, S., & Le Boudec, J. Y. (2002). Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing* (pp. 226-236).

Chen, H. (2012). RASN: Resist on-off attack for wireless sensor networks. In *Proceedings of the 2nd International Conference on Computer Application and System Modeling*.

Chen, H., Wu, H., Zhou, X., & Gao, C. (2007). Agent-based trust model in wireless sensor networks. In *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)* (Vol. 3, pp. 119-124). IEEE.

Chen, S., Zhang, Y., Liu, Q., & Feng, J. (2012). Dealing with dishonest recommendation: The trials in reputation management court. *Ad Hoc Networks, 10*(8), 1603-1618.

Clausen, T., & Jacquet, P. (2003). *Optimized link state routing protocol (OLSR)* (RFC 3626). IETF.

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering, 19*(5), 92-95.

Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN), 4*(3), 1-37.

Gupta, J. (2025). A comprehensive review of trust and reputation-based routing protocols in wireless sensor networks (WSNs): Models, challenges, and future directions. *Eksplorium-Buletin Pusat Teknologi Bahan Galian Nuklir, 46*(1), 294-300.

Haas, Z. J., & Pearlman, M. R. (2000). Providing ad-hoc connectivity with the reconfigurable wireless networks. In *Ad Hoc Networks*. Addison Wesley Longman.

Hamma, T., Katoh, T., Bista, B. B., & Takata, T. (2006). An efficient ZHLS routing protocol for mobile ad hoc networks. In *17th International Workshop on Database and Expert Systems Applications (DEXA'06)* (pp. 66-70). IEEE.

Hartman, J. H., Murdock, I., & Spalink, T. (1999). The Swarm scalable storage system. In *Proceedings 19th IEEE International Conference on Distributed Computing Systems* (pp. 74-81). IEEE.

Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In *Mobile Computing* (pp. 153-181). Springer.

Khedim, F., Labraoui, N., & Lehsaini, M. (2015). Dishonest recommendation attacks in wireless sensor networks: A survey. In *2015 12th International Symposium on Programming and Systems (ISPS)* (pp. 1-10). IEEE.

Labraoui, N., Gueroui, M., & Sekhri, L. (2015). On-off attacks mitigation against trust systems in wireless sensor networks. In *IFIP International Conference on Computer Science and its Applications* (pp. 406-415). Springer.

Labraoui, N., Gueroui, M., & Sekhri, L. (2016). A risk-aware reputation-based trust management in wireless sensor networks. *Wireless Personal Communications, 87*(3), 1037-1055.

Madisetti, V. (2016). Blockchain platform for industrial Internet of Things. *Journal of Software Engineering and Applications*, *9,* 533-546.

Michiardi, P., & Molva, R. (2002). CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Advanced Communications and Multimedia Security: IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security* (pp. 107-121). Springer.

Moeinaddini, E., Nazemi, E., & Shahraki, A. (2025). A new approach on self-adaptive trust management for social Internet of Things. *Computer Networks, 263*, 111187.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://www.klausnordby.com/bitcoin/Bitcoin_Whitepaper_Document_HD.pdf

Navaei Tourani, A., Haj Seyyed Javadi, H., Navidi, H., & Sharifi, A. (2025). A study on trust-rating mechanism for WSN node sensors using evolutionary game theory. *The Journal of Supercomputing, 81*(2), 401.

Othmen, S., Rekik, M., Zarai, F., Belghith, A., & Kamoun, L. (2016). Shortest and secure routing protocol for multi-hop cellular networks (SSRP-MCN). *Security and Communication Networks, 9*(18), 5346-5362.

Oztoprak, A., Hassanpour, R., Ozkan, A., & Oztoprak, K. (2024). Security challenges, mitigation strategies, and future trends in wireless sensor networks: A review. *ACM Computing Surveys, 57*(4), 1-29.

Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing* (RFC 3561). IETF.

Perkins, C. E., & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *ACM SIGCOMM Computer Communication Review, 24*(4), 234-244.

Pourtahmasbi, P., & Nojoumian, M. (2022). Analysis of reputation-based mining paradigm under dishonest mining attacks. *Blockchain: Research and Applications, 3*(2), 100065.

Rodrigues, P., & John, J. (2020). Joint trust: An approach for trust-aware routing in WSN. *Wireless Networks, 26*(5), 3553-3568.

Saleh, L., Taleb, A. A., & Salameh, W. A. (2020). Trust and reputation in wireless sensors networks. In *2020 21st International Arab Conference on Information Technology (ACIT)* (pp. 1-6). IEEE.

Szabo, N. (2017). Winning strategies for smart contracts. *Blockchain Research Institute*. https://grazielabrandao.wordpress.com/wp-content/uploads/2019/06/g86cmijoeemm8wp4g3tktg_1c16c8a028ce11e999f58be72bb04114_szabo-smart-contracts-v6d_1_.pdf

Tenhundfeld, N., Demir, M., & de Visser, E. (2022). Assessment of trust in automation in the "real world": Requirements for new trust in automation measurement techniques for use by practitioners. *Journal of Cognitive Engineering and Decision Making, 16*(2), 101-118.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM, 59*(11), 15-17.

Yan, Y. (2022). The overview of elliptic curve cryptography (ECC). In *Journal of Physics: Conference Series* (Vol. 2386, No. 1, p. 012019). IOP Publishing.

Yilmaz, S., & Dener, M. (2024). Security with wireless sensor networks in smart grids: A review. *Symmetry, 16*(10), 1295.

Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications, 35*(3), 867-880.

Zhang, B., Huang, Z., & Xiang, Y. (2014). A novel multiple-level trust management framework for wireless sensor networks. *Computer Networks, 72*, 45-61.

Zhang, J. (2025). WSN network node malicious intrusion detection method based on reputation score. *Journal of Cyber Security and Mobility, 12*(1), 55-76.

Zouridaki, C., Mark, B. L., Hejmo, M., & Thomas, R. K. (2009). E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks. *Ad Hoc Networks, 7*(6), 1156-1168.

Author(s) Information

Farah Khedim
University Centre of Maghnia, Route de Zouia, N99, Chouhada District, Maghnia, Tlemcen, Algeria
Contact e-mail: *f.khedim@cu-maghnia.dz*

Nabila Labraoui
University of Tlemcen
P.O.Box 230, chetouane, Tlemcen 13000, Algeria

Ado Adamou Abba-Ari
Saint-Quentin-en-Yvelines University/ University of Maroua
45 Avenue États-Unis 78035 Versailles cedex, France/ P.O. Box 814 Maroua, Cameroon

To cite this article:

Khedim, F., Labraoui, N., & Abba-Ari, A. A. (2025). B-Smart: A robust reputation-based blockchain scheme in wireless sensor networks. *The Eurasia Proceedings of Science, Technology, Engineering and Mathematics (EPSTEM), 38,* 771-790.