Available online at: http://www.ijmtst.com/vol5issue06.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 05, Issue No: 06, June 2019

Securing Wireless Sensor Network against Pollution attack with Block Chain

Komal Shinde[1] | Dr. Sachin V Todkari[2]

[1]PG Scholar, Department of Computer Engineering, JSCOE, Hadapsar, Pune, India.
[2]Associate Professor, Department of Computer Engineering, JSCOE, Hadapsar, Pune, India.

To Cite this Article
Komal Shinde and Dr. Sachin V Todkari, "Securing Wireless Sensor Network against Pollution attack with Block Chain", *International Journal for Modern Trends in Science and Technology*, Vol. 05, Issue 06, June 2019, pp.-40-47.

Article Info
Received on 12-May-2019, Revised on 09-May-2019, Accepted on 15-June-2019.

ABSTRACT

Recently, there was a massive interest to initiate security solutions in WSNs because of their applications in both civilian and military domains. Opponents can introduce different types of attacks, and block chain is used to resisting these attacks. We address the problem of pollution attacks in wireless sensor network. In a pollution attack, the opponent maliciously change some of the stored encoded packets, which are results in the incorrect decoding of a large part of the original data on retrieval. We present algorithms to detect and recover from such attacks. In contradiction to existing approaches to solve this problem, our technique is not based on adding cryptographic checksums or signatures to encoded packets, and it does not launch any additional redundancy to the system. The reason for the interest in block chain is its intermediate attributes that provide security, anonymity and data integrity without any other party organization in control of the transactions, and therefore it creates interesting research areas, particularly from the point of view of technical challenges and limitations.

KEYWORDS: *Wireless Sensor Networks (WSNs), Network Security (NS), Block Chain, Pollution Attack.*

I. INTRODUCTION

In wireless sensor network of a packet, mixing makes network coding systems endangered to a severe security threat known as pollution attacks, in which attackers introduce corrupted packets into the network. Although packet injection is not a new attack, its impact on network coding is harmful. Specifically, as long as there is one corrupted packet that an intermediate node uses during the coding process, then all the packets that are coded and forwarded by the node will be corrupted. The result is an epidemic propagation of corrupted packets, as other nodes code and forward more corrupted packets.

Traditional countermeasures to pollution attacks generally build upon malicious nodes identification and blacklisting. First, malicious nodes are discovered for example via ad-hoc coding schemes or cryptographic approaches, e.g.[1]. Second, malicious nodes are restrained from further polluting the network via, for example, blacklisting by a central authority. With random NC, it is challenging to tell whether the source of a polluted packet is a malicious node that polluted it on purpose or an honest node that accidentally relayed a polluted packet (assuming that polluted

packets could be identified in the first place). For example, cryptographic and coding complexity represents a drawback when dealing with mobile users. Similarly, the requirements for a central authority become problematic when distributing video contents to a large users population.

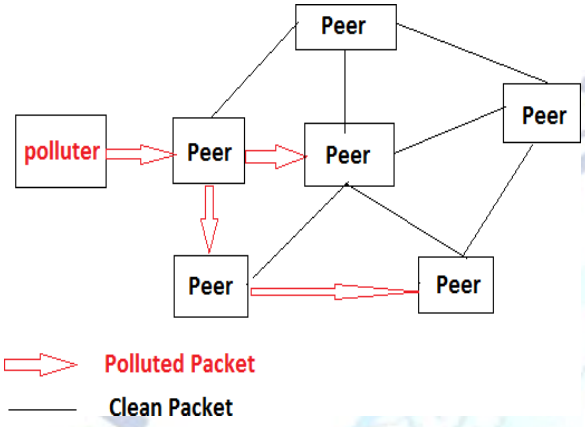

Fig. 1. pollution attack

A block chains widely used and accepted technology in cryptocurrency due to its security features. Blockchains which are readable by the public are more widely used by cryp- tocurrencies. Private block chains have been proposed for business use. Each block holds a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is against, to modification of the data. It is an open, distributed registry that can record transactions between two parties well organized and in a justified and permanent way. For use as a distributed registry, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks[2].There are 3 main types of blockchains: (1) public - per- missionless, (2) private - permission, and (3) consortium blockchains. The permission less blockchain type highlights the public part, hence all the blockchain data is accessible and vis ible to the public. However, some parts of the block chain could be encrypted in order to maintain a participants anonymity. Furthermore, in these public blockchain types, everyone can join a network as a network node. Examples of such a blockchain are Bitcoin and Ethereum block chains. In contrary, a private block chain validates only chosen nodes to join the network, thus being regarded as a form of a distributed but still centralized network. The consortium blockchain is a mixture of the two and validates only a selected group of nodes to participate in the distributed consensus process [2].

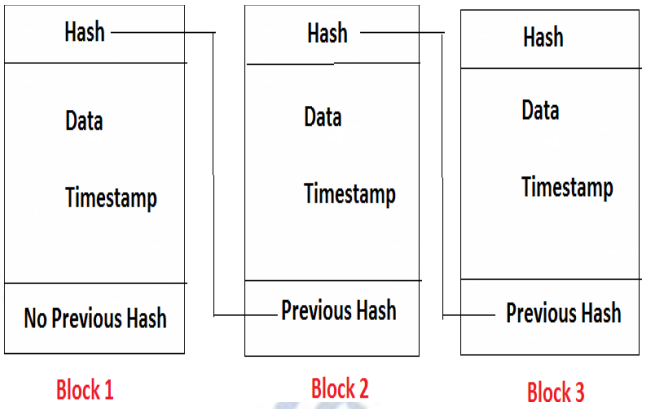

Fig. 2. Block Chain

Blockchain technology enables the creation of a decentral- ized environment where transactions and data are not under the control of any other party organization. Any transaction completed is recorded in a public ledger in a verifiable and permanent way. Blockchain technology aims at creating a decentralized environment where no third party is in control of the transactions and data. It is used in various domains due to its benefits in distributed data storage and the possibility of audit trails. With respect to other applications, media distribution can tolerate the loss of a few coding units, so perfect security of the communication may not be necessary.

In detail, the key highlights of the scheme we propose in this work are:

- it is totally distributed, so no central authority is needed;
- it is lightweight, since it requires no cryptographic com- putations and enjoys the low decoding complexity of BC;
- it is suitable for real-time communications to mobile devices;
- its ability to identify malicious nodes does not decrease as the malicious nodes inject more polluted packets into the network for the values of pollution intensity considered.

The structure of the paper is as follows. The introduction section presents in detail the motivation and the contribution of the paper. projects and research in the field related to this study, while the existing introduces the present work. The concept of the project, covers the technical parts,.e. implementation, functioning, real-life example, etc. Some reflections and issues of the work are described in detail in the discussion section. Finally, the Conclusion and

Future work provides a summary of the proposed solution and some future plans.

II. Related Works

Sr. No	Title	Author	Year of Publication	Technique Used	Advantages	Disadvantages
1	Securing Network Coding Architectures against Pollution Attacks with Band Codes	Attilio Fiandrotti, Member, IEEE, Rossano Gaeta, Marco Grangetto, Senior, IEEE	2018	Band Codes	Distributed scheme to identify and blacklist malicious nodes in video communicati on	While transmitting packet calculates honest score so it is time consuming process.
2	EduCTX: A Blockchain-Based Higher Education Credit Platform	Muhamed Turkanović , Marko Hölbl , Kristjan Košič,Marjan Heričko, And Aida Kamišalić	2018	Block chain	The proposed solution is based on the distributed P2P network system.	Not tested in real time environment.
3	Efficient and Privacy-Preserving Outsourced Calculation of Rational Numbers	Ximeng Liu,Kim-Kwang Raymond Choo ,Robert H. Deng, Rongxing Lu,Jian Weng	2016	Secure Division Protocol (SDIV), Secure Greatest Common Divisor Protocol(SGC D)	A user can securely outsource the storing and processing of rational numbers to a cloud server.	Framework which is use for calculating rational numbers is cant upload real time it only based on simulation
4	An Efficient Privacy-Preserving Outsourced Computation over Public Data	Ximeng Liu,Robert H. Deng,Yingjiu Li	2015	Message Pre-Coding Technique, Message Extending and Coding Technique (MEC)	This framework is efficient in both computation and communicati ons	It does not provide verification on outsourced computation over public database.
5	Enabling Fine grained Multi keyword Search Supporting Classified Sub dictionaries over Encrypted Cloud Data	Hongwei Li,Yi Yang,Tom H. Luan , Xiaohui Liang ,Liang Zhou , Xuemin (Sherman)Shen	2015	Fine- grained multi keyword search	By using fine grained multi keyword search schemes over encrypted cloud data we can easily search encrypted data over cloud server.	This system can't be applied on extensible file set and on multi user cloud environment.

Fig. 3. Literature Survey

Fiandrotti et al. [1] proposed a distributed scheme to identify and blacklist malicious nodes in video commu- nications leveraging on multiple properties of Band Codes (BC).While transmitting Packet, existing algorithm calculates honest score so it is a time-consuming process. Existing algorithm increases the burden on resources. At the time of communication, if an attacker changes data then a system cannot understand which packet is malicious. Muhamed Turkanovi et al. [2] have introduced a solution which is based on the distributed P2P network system. It transfers higher education grading system from the current real-world physical records or traditional digital ones (e.g. databases) to an efficient, simplified, ubiquitous version, based on blockchain technology. Limitation of this solution is it is not tested in a real-time environment. The proposed platform is based on the ECTS grading system instead of a credit system. Ximeng Liu et al. [3] implemented Secure Division Protocol (SDIV), Secure Greatest Common Divisor Protocol (SGCD) an algorithm to achieve the security in the wireless sensor network.Using this technique called POCR i.e. privacy- pre- serving outsourced calculation of rational numbers, a user can securely outsource storing and processing of rational num- bers to a cloud server without compromising the security of (original) data and the computed results. Also, it uses Paillier cryptosystem with threshold decryption (PCTD), to reduce the private key exposure risk in POCR. But this technique has one limitation i.e. A framework which is used for calculating rational numbers is cant upload real time it only based on simulation.

6	An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid	Hongwei Li,Rongxing Lu,Liang Zhou,BoYang,Xuemin (Sherman) Shen	2013	Replay attack detection	By using an efficient authenticatio n scheme, it resist the replay attack, the message injection attack.	It makes use of an approach which make system more efficient and cost effective.
7	Analysis of a Prediction-based Mobility Adaptive Tracking Algorithm	Jennifer Yick,Biswanath Mukherjee, Dipak Ghosal	2005	Prediction-based Mobility Adaptive Tracking (PMAT)	By using Kalman filtering we can make advance resource reservation coupled with adaptively changing the size of active tracking region.	This system is costly
8	Wireless Sensor Network for Habitat Monitoring: A Counting Heuristic	Erick Stattner,Nicolas Vidot,Philippe Hunel,Martine Collard	2012	Heuristic for Counting of Individuals	By using counting algorithm we can count f singing birds in their habitat by using wireless sensors fitted with microphone by which we can count species of birds.	This sensor networks generate noise when population increase.

Fig. 4. Literature Survey

Ximeng Liu et al. [4] implemented Message Pre-Coding A technique, Message Extending and Coding Technique (MEC) to improve the privacy of data over public data. This frame- work is efficient in both computation and communications. Also Because of two encryption techniques used in this paper message precoding and message extending and coding respectively, data get more secure. Only the disadvantage of An epic framework is that it does not provide verification on outsourced computation over a public database.

Hongwei Li et al. [5] proposed Fine- grained multi keyword search approach over encrypted data. As this paper uses fine- grained multi keyword search schemes over encrypted cloud data, it can easily search encrypted data over cloud server. This scheme also achieves the best security level and performance in terms of functionality, query complexity and efficiency. This system cannot be applied on extensible file set and on multi- user

cloud environment. Also, this search scheme is not that much efficient on a large practical database.

Hongwei Li et al. [6] implemented efficient Merkle tree based authentication scheme for a smart grid, Replay attack detection technique is used. Because of the use of an efficient authentication scheme, it resists the replay attack, the message injection attack, the message. It makes use of an approach which makes the system more efficient and cost-effective.

Sr. No.	Title	Author	Year	Technique Used	Advantage	Disadvantage
9	Energy and Memory Efficient Clone Detection in Wireless Sensor Networks	Zhongming Zheng, Anfeng Liu	2015	Energy efficient ring based clone detection protocol (ERCD)	The performance of the ERCD protocol evaluate in terms of clone detection probability , power consumption , network lifetime and data buffer capacity. 2)Extensive simulation results demonstrate that in the system clone detection probability and network lifetime with reasonable data buffer capacity.	1)ERCD protocol required some additional data buffer comparing with RED and P-MPC protocol. 2)Only the ring structure is consider in this paper.
10	A Trigger Identification Service for Defending Reactive Jammers in WSN	Ying Xuan, Yilin Shen, Nam P. Nguyen, and My T. Thai	2012	trigger-identification procedure	1)It provide a complete trigger identification service framework for unreliable WSN 2)It enhance the robustness of n/w	1)Identification latency is very small. 2)It would not be efficient towards jammer that are moving at a high speed.

Fig. 5. Literature Survey

Jennifer Yick et al. [7] proposed a prediction based adaptive algorithm for tracking mobile targets is used. Because use of adaptive Kalman filtering we can make advance resource reservation combine with adaptively changing the size of the active tracking region. This scheme also reduces energy consumption for tracking without affecting the accuracy in tracking.

Erick Stattneret al. [8] proposed a network of sensors fitted with a microphone to evaluate the number of birds in their habitat. Unlike previous work, they show that method is more suited to a real environment. Indeed, the method propose could be used with sensors, whose detection area is not completely circular. a solution that is based on the exploitation of a detection graph and comparison of audio signals has demonstrated to give best results when the number of sensors is high. However, experiments have shown that a limitation could be noise that can occur on signal when the population size increases.

Zhongming Zheng et al. [9] proposed Energy efficient ring based clone detection protocol (ERCD). The performance of the ERCD protocol evaluates in terms of clone detection probability, power consumption, network lifetime and data buffer capacity. 2)Extensive simulation results demonstrate that in the system clone detection probability and network lifetime with reasonable data buffer capacity 1)ERCD protocol required some additional data buffer comparing with RED and P-MPC protocol. 2)Only the ring structure is considered in this paper.

Ying Xuan et al. [10] proposed trigger identification procedure.1)It provides a complete trigger identification service framework for unreliable WSN 2)It enhances the robustness of n/w. 1)Identification latency is very small. 2)It would not be efficient towards jammer that is moving at a high speed.

III. Existing System

In this section, we show how the existing system works:

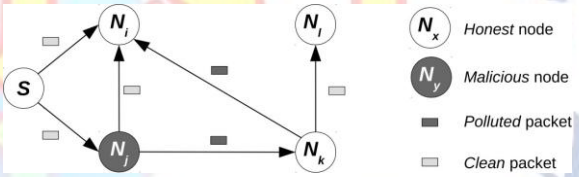

Fig. 6. Existing system

- **Pollution Attack and Propagation:** Let a network be composed of N nodes, where Nh nodes are of the honest type and Nm nodes are of the malicious type,where Nm +Nh = N.In Fig.6 the malicious node Nj relays to the honest node Nk a polluted packet. The network nodes further propagate the pollution as they do not know if a packet they received is polluted or not., in Fig. 6 the honest node Nk accidentally relays to Ni a packet which is polluted because Nk has received a polluted packet from malicious Nj.
- **Detecting Pollution Attacks:** The network nodes inde- pendently detect pollution attacks while decoding each received packet. proposed pollution detection algorithm brings several advantages.
    1) First, no additional complexity is entailed besides a bitwise comparison between the coding vectors and the coded payloads.
    2) Second, such a scheme may enable a

node to detect a pollution attack even before the generation is recovered, allowing for timely countermeasures. Third, there is a chance to detect pollution attacks at each algorithm iteration.

- **Coding to Limit Pollution Propagation:** Upon detection of a pollution attack, each node adapts its own BC parameters to limit the chances to relay polluted packets. In the case of Fig. 6, node Nj detects as pollution attack and broadcasts a warning to its neighbors including Ni. We indicate with tpoll the time at which node Ni has either detected a pollution attack or has received a warning from a neighbor. Let us assume that at time tnow ¿tpoll a transmission opportunity arises for node Ni: the difference tnow tpoll represents the time since the last evidence of a pollution attack. If lots of time has passed since the last pollution evidence, say tnow tpoll ¿ tback, Ni assumes that the attack has ended or its intensity has decreased. If tnow tpoll ¡ tback, node Ni behaves conservatively assuming that the last detected pollution attack may be still going on. So, Ni decreases the probability to relay a polluted packet.
- **Counting Polluted Packets and Exchanging Observations:** With reference to Fig. 6, node Ni has (or has had at some point in time) node Nj among its neighbors: we say that Ni has seen Nj. In the following, we indicate as Si the set of nodes are seen by Ni and as Smi the set of malicious nodes seen by Ni: clearly, Smi is a subset of Si and —Smi— indicates its cardinality. For example, in the case in Fig. 6, we have Si = Nj , Nk and Smi = Nj. We define an observation vector the vector indicating how many clean and polluted packets a node has received from each neighbor. With reference to node Ni in Fig. 6, (ci,j , pi,j) indicates the number of clean and polluted packets transmitted by Nj to Ni. Note that similarly, with reference to node Nk, (ok, j, pk,j) indicates the number of clean and polluted packets transmitted by Nj to Nk. So, the whole observation vector of Ni is Vi = (ci,j , pi,j),(ci,k, pi,k).
- **Distributed Identification and Blacklisting Scheme:** The scheme that allows a network node to independently identify and blacklist its malicious neighbors is as follows

1) As a first step, Ni immediately discards all the buffered packets received from Nj for any gener- ation. Therefore, packets received from Nj, more likely to be polluted, cannot be drawn for recom- bination and relayed any further. Next, for each generation, matrix G and vector Y are flushed and the buffered packets that were not discarded are decoded again.
2) As a second step, Nj is permanently isolated from Ni as follows. First, Ni gracefully removes Nj from its neighborhood. Second, Ni will reject any novel neighborhood request that shall come from Nj in the future. That is, Ni will not receive any coded packet directly from Nj for the rest of the communication. Assuming that Nj is similarly blacklisted by all the other nodes in the network, Nj will be isolated from the rest of the network and will be unable to relay polluted packets.

- **Reference Centralized Scheme:** On a periodic basis, the nodes envoy their observations exclusively to the tracker, that acts as a trusted central authority. Next, the tracker centrally computes a score scj for each j-th node in the network according to and permanently blacklistsnodes for which scj ¡ p. Namely, each time a blacklisted node requires novel neighbor address(es) to the tracker, the tracker ignores the request. Also, each time an honest node requires novel neighbor address(es) to the tracker, the tracker never forwards the address of blacklisted nodes. Because all the nodes periodically drop parts of their neighbors at random, malicious nodes are gradually isolated from the rest of the network.
- The existing system has various **limitations** as well:
    1) First, pollution attacks are detected only on a prob- abilistic basis, i.e. the reception of one or more polluted packets may go unnoticed.
    2) Second, it is not possible to understand which packet(s) is (are) polluted, so the node shall assume that all the packets received so far for the generation are polluted.

IV. Proposed Method

In this section, we show how the Proposed system works:

The proposed architecture is divided into five modules shown in below figure.

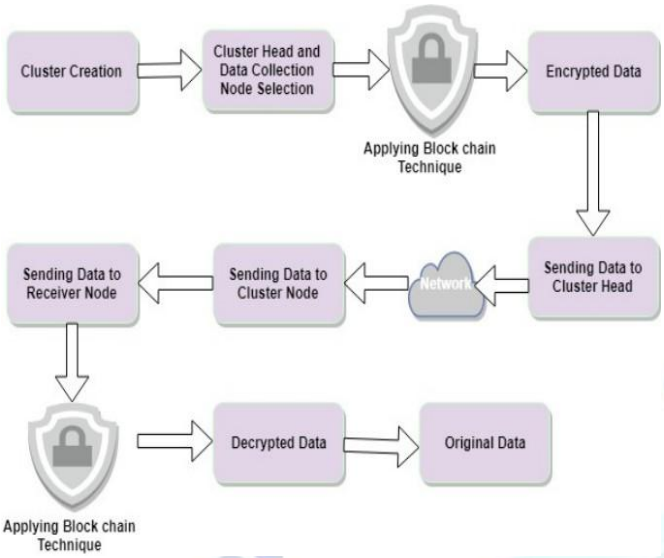

Fig. 7. Proposed System

- **Node Deployment:** System ask User to enter no of nodes to deploy. Deployed Nodes are mobile/Dynamic nodes(continuously moving).
- **Cluster Formation:** In the cluster formation module, the specific number of a node which is given by user created to form a cluster with that number of nodes. Cluster formation is based on a distance between receiver node and sensor node as well as one sensor node to another sensor node. Sensor nodes which are close to each other form one cluster. Sensor node from the same cluster has the same properties and behaviours.
- **Cluster Head Selection: :**In cluster Head selection stage, the network is divided into four clusters and each cluster has its own cluster head. Cluster head selection is based on node energy, distance from the base station and energy required for transmitter and receiver. The selected cluster head is close to the base station as well as to another sensor node. Cluster head collects sensed data from sensor nodes. It sends aggregated data to the base station. Since it is close to the base station it consumes less time, energy and power.
- **Packet transmission using Blockchain:** Each packet contains n number of blocks like data, sender and receiver etc. we will calculate the hash value of each block and this hash value is stored in the previous node and next node like a doubly linked list. If an attacker doing some changes in the packet then the hash will be changed. For calculating a hash value, we are using the SHA256 algorithm. We consider or identify nearby nodes of the sender and check its a trusty sender or not. Falsy data checked before sending to the base station. If data found to be false it will not send to the base station.
- **Receiving Data at receiver side:** Once data is received at the receiver node, the blockchain technique is applied to decrypt the received data and to convert it to original form. Finally, unaltered(original) data stored at the receiver side.

V. Mathematical Model

Set theory: Let S = N, C, CH, B, CN, A Where,

1) Deploy Sensor nodes. N= N1, N2, ..., Nn, N is set of all deployed sensor nodes.
2) Cluster formation. C= C1, C2, ..., Cn, C is a set of all clusters.
3) Select the Cluster Heads that is an aggregator for each cluster. CH= CH1, CH2, ..., CHn, CH is the set of all cluster heads.
4) Create Base Station. B= B1, B2, ..., Bn, B is a set of all base stations.
5) Find out pollution attack CN= CN1, CN2, ..., CNn, CN is a set of polluted nodes.
6) Preventing mechanism from pollution attack A= A1, A2, ..., An, A is a set of all techniques used for prevention.

VI. System Requirements

Hardware Requirements

- Hard Disk : Minimum 8 GB
- RAM : Minimum 2 GB
- Processor : Intel Pentium 4 and above.

Software Requirements

- Technology Used : Java
- Tools : JDK 1.7 or above
- IDE : Eclipse
- Operating System : Windows 7 or above.

VII. Algorithm

Algorithm: Blockchain

Input: no of nodes
Output: data send to base station.

A. Construction :

1) Sending packets/data are divided into blocks.
2) iterate each block and calculate the hash value. int temp
   for i =
   n if(i
   == 0)

temp =SHA (Data Block);
construct linked list

create node node[i] and set default address location (nodeAddress=0) ;

else

create the node and assign previous hash as an address location;

temp = SHA (Data Block);

3) linked list send to Base station.

B. Verification:

1) collect the linked list and iterate each node. int tempHash

for j = n if (j == 0)

collect data block from node[j] and calculate SHA (Data Block) tempHash = SHA (Data Block) ; else

collect data block from node[j] and calculate SHA (Data Block)

if (tempHash != current node address location) packet rejected;

else

tempHash = SHA (Data Block) ;

VIII. Results and Discussions

In this section, we first define the scenario we consider showing how pollution propagates depending on BC parameters and blockchain parameters. Afterward, we exploit the model to predict the performance of the proposed identification method. Finally, we used the actual prototype to both validate the model prediction and to analyze the effects of protocol parameters on the accuracy of the identification technique.

We consider a network with N=100 nodes where Nm = 20 are malicious and Nh = N Nm = 80 are honest. The neighborhood of each node is constrained to Ns = 5 nodes and each malicious node alters the payload of each transmitted the packet with probability ppoll = 1pecentage. Let us define the pollution overhead po as the fraction of relayed packets that are polluted. Only 20 nodes out of 100 are malicious, and each malicious node pollutes on average 1percentage of the transmitted packets, so the pollution overhead due to the malicious nodes activity amounts to just 0.02percentage of the overall traffic.

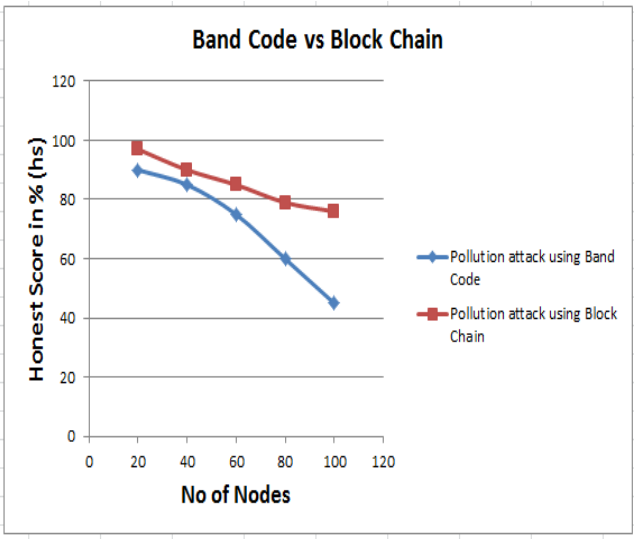

Fig. 8. Computed honest scores for different Technology

Fig 8. shows the model we developed allows us to predict the value of the honest score estimated by each node. As already discussed this amounts at estimating the system-wide parameters sh and sp. proposed identification mechanism is able to discern honestly from malicious in the long term. As a second experiment, we assess how precise is our a scheme in identifying the malicious nodes as the True Positives Ratio (TPR) of the nodes identified as malicious. For each i-th network node, we define the TPR as the fraction of true malicious nodes among the top —Smi— nodes in the sorted scores a list, where —Smi— is the subset of malicious nodes actually seen by the i-th node Namely, we study the effect of the nodes observation time to and the number of observations No available at a node.

As a general trend, malicious nodes are identified with increasing precision (i.e., the TPR increases) as No increases. However, the precision of the BC scheme increases linearly only with No: even with No=200 observations available at each node, the TPR barely exceeds 50percentage. With BC, honest nodes relay a lot of polluted packets. Thus, collected observations are unreliable and useless to discriminate between the honest and the malicious nodes. On the contrary, the blockchain schemes precisely identify (TPR between 90percentage and 100percentage) the malicious nodes with just about No = 100 observations. With Block Chain, honest nodes relay fewer polluted packets. Thus, observations

are more reliable, enabling to precisely identify malicious nodes. we study the effect of an increase of the probability ppoll that a malicious node injects a bogus packet. We show the precision in malicious identification (TPR) as ppoll increases above 1percentage. As expected, the experiments confirm that the honest nodes relay more polluted packets to the network as ppoll increases. With BC, the TPR drops as ppoll increases: as malicious nodes inject more polluted packets, the ambiguity between honest and malicious nodes increases and collected observations are less discriminative to identify the malicious nodes. On the contrary, with Blockchain the TPR increases as ppoll increases: malicious nodes are in fact more likely to be correctly identified when they transmit more polluted packets to the network.

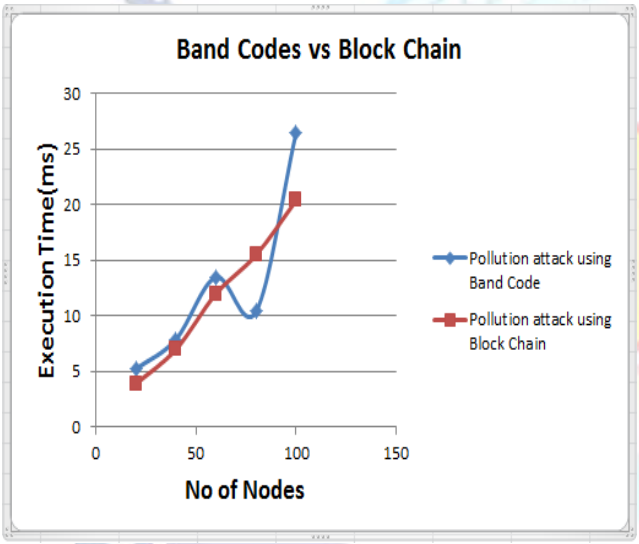

Fig. 9. Computed Execution Time for different Technology

Fig. 9. Shows shows that, with our proposed a scheme, injecting more polluted packets in the network may be counterproductive for malicious nodes as they are more easily identified and isolated from the network.

IX. Conclusion and Future Work

We addressed the problem of pollution attack in coding- based distributed storage schemes, and we proposed specific algorithms for detecting and recovering from such attacks. A salient feature of the proposed algorithms is that they are not based on cryptographic checksums or digital signatures, which are traditionally used for providing integrity services. Instead, we take advantage of the blockchain technology in such distributed storage systems. In particular, our approach is to obtain more encoded packets than strictly necessary for the decoding of the original data and to use those additional encoded packets for attack detection and recovery purposes. By not using cryptography, we do not need to rely on a PKI or preestablished secure channels, which are the usual drawbacks of the alternative approaches. The attack detection algorithm that we will propose in the project will effective and extremely efficient both in terms of communication and computational overhead. We will try to implement this simulated results over real-time wireless sensor network. We will overcome the issue of various attacks takes place while transactions in the banking and financial sectors by using this blockchain technology.

References

[1] Attilio Fiandrotti, Rossano Gaeta, Marco Grangetto, Securing Net- work Coding Architectures against Pollution Attacks with Band Codes", IEEE Transactions on information forensics and security, July 2018.

[2] Muhamed Turkanovic, Marko Holbl, Kristjan Kosic, Marjan Her- icko and Aida Kamisalic, EduCTX: A blockchain-based higher education credit platform", IEEE ACCESS, VOL. X, NO. Y, 2017.

[3] Ximeng Liu,Kim-Kwang Raymond Choo ,Robert H. Deng, Rongx- ing Lu,Jian Weng, Efficient and Privacy-Preserving Outsourced Calculation of Rational Numbers", IEEE Transactions on Depend- able and Secure Computing, 2015.

[4] Ximeng Liu,Baodong Qin, Robert H. Deng, Yingjiu Li, "An Efficient Privacy-Preserving Outsourced Computation over Public Data", IEEE Transactions on Services Computing, 2015.

[5] Hongwei Li, Yi Yang, Tom H. Luan, Xiaohui Liang, Liang Zhou and Xuemin (Sherman) Shen, "Enabling Fine-grained Multi- keyword Search Supporting Classified Sub-dictionaries over En- crypted Cloud Data", IEEE Transactions on Dependable and Secure Computing, 2015.

[6] Hongwei Li, Rongxing Lu, Liang Zhou, Bo Yang, and Xuemin (Sherman) Shen, "An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid", IEEE SYSTEMS JOURNAL, 2013.

[7] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal yick, mukherje, ghosal, "Analysis of a Prediction-based Mobility Adap- tive Tracking Algorithm", IEE, 2005.

[8] Erick Stattner, Nicolas Vidot, Philippe Hunel and Martine Collard estattne, nvidot, phunel, mcollard, "Wireless Sensor Network for Habitat Monitoring: A Counting Heuristic", 12th IEEE Interna- tional Workshop on Wireless Local Networks, 2012.

[9] Zhongming Zheng, Anfeng Liu, Lin X. Cai, Zhigang Chen and Xuemin (Sherman) Shen, "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks", IEEE Transactions on Mobile Computing, 2015

[10] Ying Xuan, Yilin Shen, Nam P. Nguyen, and My T. Thai, "A Trigger Identification Service for Defending Reactive Jammers in WSN", A Trigger Identification Service for Defending Reactive Jammers in WSN, VOL. 11, NO. 5, MAY 2012.