M2M-REP: Reputation of Machines in the Internet of Things

Muhammad Ajmal Azad
School of Computing Science
Newcastle University
Newcastle Upon Tyne, UK
muhammad.azad@ncl.ac.uk

Samiran Bag
School of Computing Science
Newcastle University
Newcastle Upon Tyne, UK
samiran.bag@ncl.ac.uk

Feng Hao
School of Computing Science
Newcastle University
Newcastle Upon Tyne, UK
feng.hao@ncl.ac.uk

ABSTRACT

The Internet of Things (IoT) is the integration of a large number of autonomous heterogeneous devices that report information from the physical environment to the monitoring system for analytics and meaningful decisions. The compromised machines in the IoT network may not only be used for spreading unwanted content such as spam, malware, viruses etc, but can also report incorrect information about the physical world that might have a disastrous consequence. The challenge is to design a collaborative reputation system that calculates trustworthiness of machines in the IoT-based machine-to-machine network without consuming high system resources and breaching the privacy of participants. To address the challenge of privacy preserving reputation system for the decentralized IoT environment, this paper presents a novel M2M-REP (Machine to Machine Reputation) system that computes global reputation of the machine by aggregating the encrypted local feedback provided by machines in a fully decentralized and secure way. The privacy of participating machines is well protected such that machines or analyst would not learn any information about the feedback score provided by the participating machines other than the final aggregated statistical score. We present a decentralized reputation aggregation system for two scenarios: a semi-honest (honest-but-curious) setup where machines are trustworthy in providing feedback but are curious to learn sensitive information about the collaborating machines, and the malicious model where machines not only try to learn the sensitive information of participants but also do not follow the protocol specification in providing feedback. We analyzed the security and privacy properties of the M2M-REP system for different adversarial models.

CCS CONCEPTS

• **Computer systems organization** → *Network Security*; Internet of Things, Machine 2 Machine; • **Networks** → Network Security, Privacy;

KEYWORDS

Machine 2 Machine, Decentralized Reputation, Privacy Protection, Secure Computation, Trust

ARES '17, Reggio Calabria, Italy

DOI: 10.1145/3098954.3098976

ACM Reference format:
Muhammad Ajmal Azad, Samiran Bag, and Feng Hao. 2017. M2M-REP: Reputation of Machines in the Internet of Things. In *Proceedings of ARES '17, Reggio Calabria, Italy, August 29-September 01, 2017,* 7 pages.
DOI: 10.1145/3098954.3098976

1 INTRODUCTION

The Internet of things (IoT) is the internetwork of connected devices that are mainly used for monitoring the physical environment and reports monitored events to the administrative/analyst systems for the detailed analytics and meaningful decisions. Recent statistics on the IoT future forecast shows that there will be around 50 billion IoT devices for 7.6 billion people (around 6 devices per person) [1] around the globe. In IoT network, the things can be sensors (embedded in smartphones), machines, actuators, smart devices, smart phones or even the human beings. Machine 2 Machine (M2M) communication becomes the central part of the IoT network as machines can directly communicate with each other, and can also provide on demand value added service (video content, suggesting maps etc.) to the end-users. The M2M connections across the globe are increasing at the rate of 25% per year from 2015 to 2020 [2], and there will be more than one billion M2M devices by the year 2020.

The unprecedented growth of M2M connections has also attracted malicious users and intruders to attack the unsecured IoT devices for distributing unwanted malicious contents such as spam, malware, and viruses [3]. Moreover, the intruder could also get control of devices and sends false observations about the physical world to the central monitoring room or other machines that might have disastrous consequences. In order to provide secure services and safeguard the open Machine to Machine network to be used for malicious activities, there is a strong need to have a trusted system that can effectively identify the misbehaving machines without the use of trusted centralized system for analytics and decisions. It is important for the M2M devices to monitor the communication behavior of other devices and assign trust scores to them based on their past interaction so to identify misbehaving machines in a collaborative way [4]. The trust and reputation systems could identify the malicious machines by incorporating the collaboration among the machines in the network. However, the reputation system needs to have the following properties: 1) It must protects private information of collaborating machines, so that a large number of users participate in collaboration without having any threat to their privacy, 2) it must not require any trusted centralized system to which the feedbacks scores are exchanged for the aggregate statistics, thus performing computation in a completely decentralized fashion, and 3) it does not incur excessive system and network resources.

To address these challenges, this paper describes an M2M-REP (Machine to Machine Reputation) system that computes the trustworthy score of machines in the network by aggregating the private feedback provided by participants in a completely decentralized and secure way. To this extent, the participating machines first assign a feedback score to its directly interacted machines based on their past transactions, and second exchanges cryptogram of the feedback score to the public bulletin board. The reputation aggregator/analyst or any other machine in the network then computes the global reputation of any machine by multiplying the feedback cryptograms assigned to the machine in a multi-party computation system. Specifically, we present the system for two scenarios: 1) a semi-honest model – where machines provide honest feedback but are curious to learn the private information of participants and the relationship network of machines and its users, and 2) a malicious model – where machines provide false scores (out-of-range value) to have a high final reputation score for some machines. M2M-REP system is novel in the following aspects. First, it allows each machine to submit the feedback in one of three values – negative (-1 means non-trustworthy), positive (1 means trustworthy), or not sure (0 means not interacted)– as a cryptogram to the bulletin board. Second, it constructs an efficient zero-knowledge proof to prove that the provided feedback is either 0, 1 or -1 thus effectively exclude machines providing out-of-range value in the final reputation score. Third, the bulletin board is completely decentralized and is available all the time, thus minimizes the single point of failure. The M2M-REP system does not require participants to remain on-line during the aggregation process. The proposed approach is efficient in terms of computation and bandwidth complexity for the honest but curious model, and has slightly high computational and bandwidth overheads for the malicious model because of use of non-interactive zero knowledge proof.

The remaining part of the paper is organized as follows. Section 2 presents the representation of the M2M network as a social network of machines and formalizes the problem definition. Section 3 reviews existing work on the reputation in M2M and P2P (peer to peer) networks. We introduce the new M2M-REP system for semi-honest and malicious models in a Section 4. In Section 5 we analyze the security and privacy properties of the proposed system. Finally, we conclude the paper in Section 6.

2 PRELIMINARIES

In this section, we describe preliminaries that allow us to describe and analyze the proposed system in Section 4.

2.1 Graph Representation of M2M Network

The M2M network can be represented as a directed weighted graph network $G(N, E, W)$ as shown in a Figure 1, where N represents the identity of the machines in the network, V represents the edge between machines only if machines have interacted least once, and W represents the weighted trust relationship between machines based on their past transactions history. The edge can be either directed inwards (machines providing services) or can be directed outward (machine asking for the services). In a directed graph the sum of inward edges and outward edges is termed as an in-degree and the out-degree of the nodes. The weights on edges between

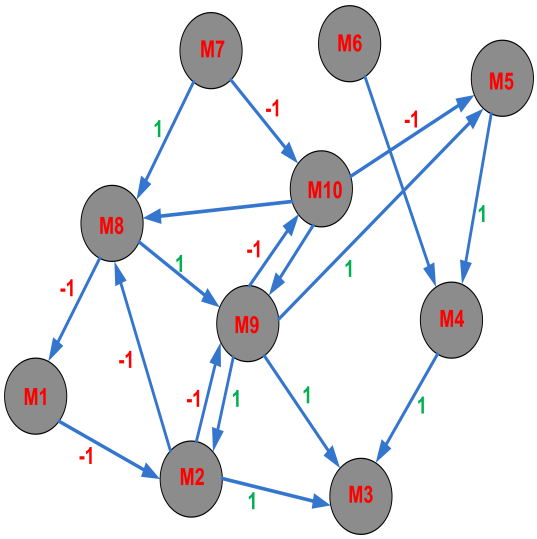

Figure 1: The representation of M2M Network as a Graph Network with local trust scores 1 and -1.

nodes are computed after the completion of a transaction and can be either 1 (trusted interaction), -1 (untrusted interaction) or 0 (uncertain or no interaction). The graph presented in a Figure 1 can be represented as a sparse adjacency matrix.

$$M_{ij} = \begin{cases} connected; & \text{if } N_i \text{ interacted } N_j \\ non-connected; & \text{Otherwise} \end{cases} \quad (1)$$

2.2 Problem Statement

Suppose there is a M2M network of n $(N1, N2, \ldots, N_n)$ machines interacting with each other. Each machine in a network evaluates the trustworthiness of it's directly interacted machines and assigns direct trust based on the outcome of transactions. Consider a trust matrix $M = (v_{ij})$, where $(i, j) \in N$, v_{ij} is the direct trust score assigned by the machine i to the machine j. The direct trust matrix can be represented as a matrix:

$$M = \begin{pmatrix} v_{11} & v_{21} & v_{31} & \cdots & v_{n1} \\ v_{12} & v_{22} & v_{32} & \cdots & v_{n2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{1n} & v_{2n} & v_{3n} & \cdots & v_{nn} \end{pmatrix} \quad (2)$$

The trust value v_{ij} assigned by the machine N_i to machine N_j can have one of the following three values:

$$v_{ij} = \begin{cases} -1; & \text{if Machine is not trustworthy} \\ 1; & \text{if machine is trustworthy} \\ 0; & \text{if the status is uncertain or not interacted} \end{cases} \quad (3)$$

There are some machines that want to have interactions with unknown machines; however, without having any information about the behavior (reputed or non-reputed) of a machine towards others, the machine may hesitate to have interaction with the unknown machine because of fear of receiving malicious content from the untrusted machines. There is a global trust vector representing the global reputation or global trustworthy scores of machine

$R = (t_1, t_2, \ldots, t_n)'$ such that each $t_i \in [1, h], \forall i \in [n]$, h being a small integer. The global trust vector represents the aggregate trustworthiness of machine as perceived by machine behavior towards other machines. The problem is to compute the global trust vector of the machine by aggregating the feedback score assigned to the machine by other interacted machines in a completely secure and private way. The challenges in the design of such reputation aggregation system for distributed M2M network are three folds: 1) the computation complexity and communication overheads required for computing the global reputation should be small, 2) the reputation aggregation process ensures that the privacy of machines taking part in providing feedback is well protected, that is the local feedback provided by machines would not be revealed to any other entity, and 3) the feedback of machines should also be included in a final reputation aggregation process even if the machine is off-line at the time of the aggregation process.

2.3 Adversary

In this paper, we develop a system for the honest but curious machines and the malicious machines models. Honest but curious machines operate according to the protocol specification, always provide honest feedback to the bulletin board, however, these machines try to infer the feedback values provided by the participants. Further, adversary in curious model also try to infer the relationship network of participants i.e. who communicates with whom. The malicious adversary model has two objectives: 1) participants do not provide the honest feedback (for example, provide out-of-range high or low feedback values to machines in order to make the aggregation incorrect), and 2) adversary in this model try to infer relationship network and feedback scores of target participants.

2.4 Privacy

Privacy in M2M reputation systems is twofold; 1) the feedback or data provided by the collaborators is not revealed to any other trusted third party system or participating collaborators, 2) the feedback scores are encrypted such that they cannot be used to infer the relationship network of participating collaborators. The privacy preserving reputation aggregation protocol ensures that feedback values or private information would only provide aggregate statistics without knowing the individual feedback score. Let x be some private feedback score which is held by the machine and exchanged to the bulletin board as the input for collaboration. The bulletin board, aggregator, adversary and machines are considered as preserving the privacy of collaborating machines if no entity can learn the feedback score or infer any information apart from the aggregated reputation score of participants.

3 STATE OF THE ART

We review the literature in two aspects; first, an M2M network, and second the P2P (peer to peer) network. In M2M communication, the secure aggregation is mainly studied from the perspective of smart reading. In [5], authors proposed two trustworthiness management models for detecting the malicious objects in an IoT network. In the first model, each object computes the trustworthiness of other objects on the basis of its direct interaction, and in the second system information about each node is distributed and stored using the DHT (Distributed Hash Table) structure so that any object can have the same information for the aggregate behavior. In this approach, the direct feedback could be revealed to other machines thus disclosing social network of machines. In [6], authors proposed two approaches for protecting privacy and feedback of participating nodes while computing trust and reputation of the nodes. The first approach is based on PKC (Public Key Cryptography) and uses an additive homomorphic system to protect the integrity of feedback provided by the participating nodes, and the second approach is based on the additive pallier-crypto system. However, the efficiency of schemes relies on the trustworthiness of participating nodes i.e. nodes are honest in providing the correct feedback. The first scheme achieves better computational efficiency, while the second one provides greater security at the expense of a higher computational cost. In [7], data from the smart grid application is aggregated by having the concentrators in the neighborhood of smart grid network. In [8] authors present a decentralized auction system for the cyber-physical systems, but they have not provided any security and privacy aspects of machines participating in the auction for the specific task. In [9] authors protect the privacy of reading data by anonymizing the smart metering data, and submit it to a third party arbitrator; however, anonymized data is subject to de-anonymization by correlating information from multiple sources [10]. A non-trusted aggregator can evaluate the sum of user's feedback value without imposing any limit on the number of participants [11]; however, it requires a large number of encryption keys to manage the individual feedbacks and decryption of encrypted reputation scores. In LotS [12], the privacy and anonymity of information provided by the participating nodes are maintained using cryptographic approaches based on the voting approach. However, the approach includes the feedback from both legitimate and malicious nodes in evaluating the final trust score of the nodes.

Several decentralized and distributed systems have been proposed for reputation aggregation and management in a P2P network. In [13] a decentralized system is proposed for aggregating the reputation of users in a P2P network; a malicious user, however, can easily track activities of others by assigning specific reputation scores. In [14] a secure homomorphic crypto-based system is proposed that ensures the privacy of users while computing global reputation of the users. In [15] an Eigen trust algorithm is proposed for aggregating the feedback scores provided by peers in a decentralized P2P network. However, in Eigen trust algorithm, the scores of feedback are known to the nodes participating in the aggregation process. Furthermore, the participating nodes also know who is communicating with whom, and nodes need to remain on-line during the aggregation process. In [16, 17] a decentralized privacy preserving reputation protocol is proposed for the reputation aggregation under the malicious adversarial model. The protocol operates in two steps: first, it requires the feedback from the certain honest providers, and second, it aggregates the feedback in a decentralized manner. However, having a set of pre-trusted users is not always feasible. It is important to have a system that is not dependent on a set of pre-trusted peers. In [18], another decentralized reputation system is proposed but it requires a trusted module chip at each participating agent or peer.

Notation	Meaning
$N_1, N_2, \ldots, N_n$	machines
NIZK	non-interactive zero knowledge
G	cyclic group of p elements in which DDH problem is hard
$[n]$	the set $\{1, 2, \ldots, n\}$
$[a, b]$	the set $\{a, a+1, \ldots, b\}$
$\lfloor a \rceil$	nearest integer of a
$(x_{i1}, x_{i2}, \ldots, x_{in})$	private key of N_i
$(g^{x_{i1}}, g^{x_{i2}}, \ldots, g^{x_{in}})$	public key of N_i
$(g^{y_{i1}}, g^{y_{i2}}, \ldots, g^{y_{in}})$	restructured key of N_i
$V_i' = (v_{i1}, v_{i2}, \ldots, v_{in})'$	local trust vector of N_i
M	the matrix $[V_1 \| \| V_2 \| \| \ldots \| \| V_n]$
R	$(n \times 1)$ global reputation vector
T'	$(n \times 1)$ updated global reputation vector for next cycle

Table 1: Notations & abbreviations Used in the design of M2M-REP.

4 M2M-REP: SYSTEM FOR REPUTATION AGGREGATION IN AN IOT-BASED MACHINE TO MACHINE NETWORK

In this section, we present the architecture of an M2M-REP system and detail the procedure for aggregating the local feedback under honest-but-curious and malicious models.

4.1 System Architecture

The M2M-REP system is a decentralized system that computes reputation of machines without any third party trusted centralized system or setup. The block diagram of the M2M-REP system is presented in a Figure 2 which mainly consists of two major components: the machines that are providing services and communicating with other machines, provide feedback values; and the decentralized public bulletin board that holds encrypted feedback and the non-interactive zero-knowledge proof reported by the participating machines. The M2M-REP system requires that feedback values should be posted to bulletin board in the encrypted form such that no one having access to feedback scores can decode them to learn the actual scores of machines for the other machines. Each collaborating machine reports the encrypted score to the bulletin board and their associated non-interactive zero knowledge (NIZK) proof to prove non-interactively that feedback is indeed 1 of the three values (0,1,-1).

4.2 Protocol Description

The reputation aggregation mechanism of M2M-REP system is based on the semantics of a decentralized open-vote protocol [19], originally designed for the decentralized self enforcing and verifiable e-voting that conducts elections without trusted third party. In [19] a group of n voters secretly compute a final tally $T = \sum_{i=1}^{n} v_i$, where $v_i \in \{0, 1\}$ is the secret input of voter $V_i, \forall i \in [n]$. However, we modify the scheme presented in [19], so as to incorporate three

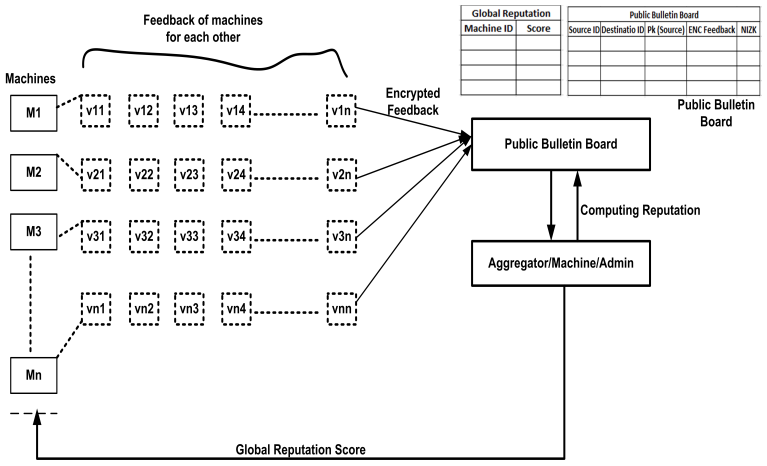

Figure 2: M2M-REP system architecture. Machines assign direct score to other machines whom they interacted. The encrypted feedback are then sent to feedback reporting bulletin board. The reputation is then aggregated without revealing the trust scores.

values that are $v_i \in \{0, 1, -1\}$, and also modify the zero knowledge proof for 3-out of one value.

4.3 Protocol Assumptions

Let G be a finite group of p elements in which Decisional Diffie-Hellman (DDH) problem is hard to compute. Let g be a random generator of G. There is a publicly accessible append only bulletin board to which the collaborating machines report their encrypted feedback and the NIZK well-formedness. A collaborating machine authenticates every message it uploads to the bulletin board by digitally signing the message. We assume that the machines have only append & read' access to the Bulletin Board (BB) over the authentic channel. Further, we assume that machines are only providing feedback for the machines whom they have interacted any time in the past.

4.4 Protocol Operations

The reputation aggregation process in a M2M-REP system consists of three steps: 1) the participating machines generate the secret and public keys, keeps the secrete key to themselves, and publish public key on the bulletin board. 2) the participating machines then first compute the restructured key from the public keys, and secondly encrypt the feedback using private key and the restructured key, and publish cryptograms along with NIZK proof to the bulletin board (BB), and 3) computing the global reputation vector by multiplying the published cryptograms. Each of these steps are detailed as under:

4.4.1 Generating Public Parameters and Providing Feedback. Let us assume there is a M2M network comprising n machines $N_1, N_2, \ldots, N_n$. Every machine $N_i, i \in [n]$ holds a feedback trust vector $V_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, where $v_{ij} \in \{-1, 0, 1\}$ as represented in equation 3. The global reputation of the machines can be represented as a vector of score $R = (t_1, t_2, \ldots, t_n)$. $t_i \in [1, h], \forall i \in [n]$. If machine is appearing for the first time, then value of t_i for such machine is

initialized with 1. In equation 2 the columns of the matrix M_{nxn} are the local trust vectors (feedback scores) held by the n machines, that is $M = [V_1||V_2||\dots||V_n]$. All the collaborating machines collaborate secretly for computing the temporary global reputation vector $R' = (R'_1, R'_2, \dots, R'_n)$, where $R'_j = \lfloor \frac{\sum_{i=1}^{n} M_{ij} * R_i}{\sum_{i=1}^{n} R_i} * (h-1) \rceil, \forall j \in [n]$. The updated global reputation vector $T' = (t'_1, t'_2, \dots, t'_n)$ for the iterative process (next aggregation cycle) can be computed as:

$$t'_i = 1 + R'_i \tag{4}$$

The *feedback phase* has two phases. In phase I, each machine $N_i, i \in [n]$ chooses a random secret key $X_i = (x_{i1}, x_{i2}, \dots, x_{in}) \in_R \mathbb{Z}_p^n$. It keeps the secret key $X_i = (x_{i1}, x_{i2}, \dots, x_{in})$ and publishes the corresponding public key $Pub_i = (g^{x_{i1}}, g^{x_{i2}}, \dots, g^{x_{in}})$ on the public bulletin board. In the second phase, each machine $N_i, i \in [n]$ computes a ballot $C_i = (c_{i1}, c_{i2}, \dots, c_{in})$, where the value of each c_{ij} is computed as following:

$$c_{ij} = g^{x_{ij} y_{ij}} g^{t_i v_{ij}} \tag{5}$$

In this phase, the machine N_i also generates $g^{y_{ij}}$, a restructured public key as following:

$$g^{y_{ij}} = \prod_{k=1}^{i-1} g^{x_{kj}} / \prod_{k=i+1}^{n} g^{x_{kj}}, \forall j \in [n] \tag{6}$$

where y_{ij} is

$$y_{ij} = \sum_{k=1}^{i-1} x_{kj} - \sum_{k=i+1}^{n} x_{kj} \tag{7}$$

$$g^{y_{ij}} = \prod_{k=1}^{i-1} g^{x_{kj}} / \prod_{k=i+1}^{n} g^{x_{kj}} \tag{8}$$

As the values of $g^{x_{ij}}$ are available publicly on the bulletin board, N_i can compute $g^{y_{ij}}$ for all $j \in [n]$ without calculating y_{ij}. Hence, machine N_i can compute c_{ij} as following

$$c_{ij} = (g^{y_{ij}})^{x_{ij}} g^{t_i v_{ij}} \tag{9}$$

The machines also provide NIZK (non-interactive zero knowledge proof) to ensure that the feedback provided by N_i is one of the three values(0,1 and -1). The NIZK proof consists of a witness to the fact that $c_{ij} \in \{g^{x_{ij} y_{ij}} / g^{t_i}, g^{x_{ij} y_{ij}}, g^{x_{ij} y_{ij}} g^{t_i}\}$. The construction of this proof is discussed in the Appendix. N_i posts on the bulletin board C_i and $PW_{ij}[\cdot]$ for all $j \in [n]$.

4.4.2 Global Reputation of Machine. Once the encrypted local direct trust of machines are reported to BB, anyone (Network Manager, aggregator, system administrator or any other machines) can compute global reputation score of the particular machine or all machines in the network as $R = (R_1, R_2, \dots, R_n)$, where the value R_i is computed as following:

$$l_j = \prod_{k=1}^{n} c_{ij} \tag{10}$$

$$= \prod_{k=1}^{n} g^{x_{kj} y_{kj}} g^{t_k * v_{kj}} \tag{11}$$

$$= g^{\sum_{k=1}^{n} x_{kj} y_{kj}} g^{\sum_{k=1}^{n} t_k v_{kj}} \tag{12}$$

$$\sum_{k=1}^{n} x_{kj} y_{kj} = \sum_{k=1}^{n} x_{kj} \Big(\sum_{m=1}^{k-1} x_{mj} - \sum_{m=k+1}^{n} x_{mj} \Big) \tag{13}$$

$$= \sum_{k=1}^{n} \sum_{m<k} x_{mj} x_{kj} - \sum_{k=1}^{n} \sum_{m>k} x_{mj} x_{kj}. \tag{14}$$

$$\sum_{k=1}^{n} \sum_{m<k} x_{mj} x_{kj} = \sum_{m,k=1,m<k}^{n} x_{mj} x_{kj} \tag{15}$$

$$= \sum_{m,k=1,m>k}^{n} x_{mj} x_{kj} \tag{16}$$

$$= \sum_{k=1}^{n} \sum_{m>k} x_{mj} x_{kj}. \tag{17}$$

As,

$$\sum_{k=1}^{n} x_{mj} y_{mj} = 0 \tag{18}$$

Thus,

$$l_j = g^{\sum_{k=1}^{n} t_k v_{kj}} = g^{u_j} \tag{19}$$

Since, $u_j \in [0, nh]$, a limited brute force search on l_j would yield u_j. Then, the aggregator can compute $R_i = \lfloor \frac{u_i (h-1)}{\sum_{j=1}^{n} t_j} \rceil$ and updates global trust vector T' for the next aggregation cycle using equation 4.

4.4.3 Feedback Verification Under Malicious Machines. The verification of correctness of the feedback received at the BB is the fundamental step of the M2M-REP system, as it prevents machine to provide extremely high and low false value about other machines in order to disrupt the system. This would also prevent malicious machines to assign high trust scores by making the artificial social circle. M2M-REP provides verification by checking the values of zero knowledge proof that provides information whether the reported local trust is −1 or 0 or 1 in a non-interactive way and without learning the value of feedback.

Each encrypted feedback is of the form $c_{ij} = g^{x_{ij} y_{ij}} g^{t_i v_{ij}}$, where $g^{x_{ij}}, g^{y_{ij}}$ is provided on the bulletin board, v_{ij} is −1 or 0 or 1, and t_i comes from the global trust vector T. Here we discuss how each machine can construct a NIZK proof $PW_{ij}[c_{ij} : g^{x_{ij}}, g^{y_{ij}}, t_j]$. This proof consists of a witness to the fact that exactly one of the three statements below is true:
1) $c_{ij} = g^{x_{ij} y_{ij}} g^{t_j}$
2) $c_{ij} = g^{x_{ij} y_{ij}}$
3) $c_{ij} = g^{x_{ij} y_{ij}} / g^{t_j}$
where $g, g^{x_{ij}}, g^{y_{ij}}$ and t_j are public. This is a 1-out-of-3 statement. Let us assume that the first statement is true, that is $c_{ij} = g^{x_{ij} y_{ij}} g^{t_j}$. Hence, the prover will have to provide a real proof for the first statement and two simulated proofs for two other statements. For the sake of clarity, we denote $c_{ij}, x_{ij}, y_{ij}, t_j$ as c, x, y and t respectively. Hence, the prover has to prove that $c = g^{xy} g^t$, or g^{xy} or $g^{xy} g^t$. The prover chooses a random $r_1 \in_R \mathbb{Z}_p$ and computes a commitment $com_1 = g^{r_1}, com'_1 = (g^y)^{r_1}$. The prover chooses random challenges $ch_2, ch_3 \in_R \mathbb{Z}_p$ and two responses $res_2, res_3 \in_R \mathbb{Z}_p$ and computes 4 commitments:
$com_2 = g^{res_2} (g^x)^{ch_2}, com'_2 = (g^y)^{res_2} c^{ch_2}$
$com_3 = g^{res_3} (g^x)^{ch_3}, com'_3 = (g^y)^{res_3} (c * g^t)^{ch_3}$

Let the grand challenge of the NIZK statement be ch. The prover calculates $ch_1 = ch - ch_2 - ch_3$. Then the prover computes a response $res_1 = r_1 - x * ch_1$.

The verification equations are as below:

(1) $g^{res_s} \stackrel{?}{=} \frac{com_s}{(g^x)^{ch_s}}, \forall s \in \{1,2,3\}$
(2) $(g^y)^{res_1} \stackrel{?}{=} \frac{com'_1}{(c/g^t)^{ch_1}}$
(3) $(g^y)^{res_2} \stackrel{?}{=} \frac{com'_2}{c^{ch_2}}$
(4) $(g^y)^{res_3} \stackrel{?}{=} \frac{com'_3}{(c*g^t)^{ch_3}}$

If these six verification equations are satisfied, then the proof is accepted. The total number of commitments of the proof is 6, the total number of responses is 3 and the total number of challenges is 3. Hence, the size of the NIZK proof is 12.

Similarly, NIZK proof can be generated for the two other cases, that is for $c = g^{xy}$ and for $c = g^{xy}/g^t$.

5 SECURITY ANALYSIS OF M2M-REP

In this section, we analyze the security and privacy properties of the M2M-REP system.

5.1 Security of M2M-REP

We analyze the security,privacy and correctness of M2M-REP system for two adversarial modes: 1) a honest-but-curious model and the malicious machine model. Additionally, the malicious machines have the ability to colludes with others machines to find the trust scores assigned by the target machines. Let us assume that the adversary $\mathcal{A}$ colluded with k ($N_1, N_2, \ldots, N_k$) number of machines. The honest machines are $\{N_i : i \in [k,n]\}$. The adversary $\mathcal{A}$ acquires the local trust values and the secret keys of the colluding machines. In a Lemma 5.1 we prove that the adversary is only able to learn the partial aggregated sum of the target honest machine i.e $\sum_{i=k+1}^{n} t_i v_{ij}$ for honest machine $j \in [n]$. Lemma 5.1 proves that M2M aggregation protocol would not allow adversary to correlate information from the colluding machines and the aggregated sum to infer the trust scores assigned by the target machine. Further, the adversary also would not be able to infer the communication network of the target machine. In nutshell, the M2M aggregation protocol in an SMC (Secure Multi-party Computation) setting achieves the maximum protection of trust scores and relationship network without the use of trusted setup and selection of trusted peers.

Lemma 5.1. *Let us assume that the adversary $\mathcal{A}$ colludes with machines in the set $S_{\mathcal{A}} = \{N_i : i \in [k]\}$ for some arbitrary k. Let,*

$$M = \begin{bmatrix} v_{11} & v_{21} & \cdots & v_{k1} & v_{k+11} & v_{k+21} & \cdots & v_{n1} \\ v_{12} & v_{22} & \cdots & v_{k1} & v_{k+12} & v_{k+22} & \cdots & v_{n2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ v_{1k} & v_{2k} & \cdots & v_{kk} & v_{k+1k} & v_{k+2k} & \cdots & v_{nk} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ v_{1n} & v_{2n} & \cdots & v_{kn} & v_{k+1n} & v_{k+2n} & \cdots & v_{nn} \end{bmatrix}$$

$$M' = \begin{bmatrix} v_{11} & v_{21} & \cdots & v_{k1} & v'_{k+11} & v'_{k+21} & \cdots & v'_{n1} \\ v_{12} & v_{22} & \cdots & v_{k1} & v'_{k+12} & v'_{k+22} & \cdots & v'_{n2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ v_{1k} & v_{2k} & \cdots & v_{kk} & v'_{k+1k} & v'_{k+2k} & \cdots & v'_{nk} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ v_{1n} & v_{2n} & \cdots & v_{kn} & v'_{k+1n} & v'_{k+2n} & \cdots & v'_{nn} \end{bmatrix}$$

Also assume that $\sum_{i=k+1}^{n} t_i v_{ij} = \sum_{i=k+1}^{n} t_i v'_{ij}, \forall j \in [n]$.The adversary $\mathcal{A}$ will not be able to distinguish between the two bulletin boards corresponding to the two sets of local trust values M and M'.

The security of the M2M-REP reputation protocol under the DDH assumption is proved from the Lemma that proves the security of multi-party computation in assumption 2 . Hence, the protocol is secure under the DDH assumption.

Assumption 1. ***[DDH assumption]*** *Given $g, g^a, g^b \in G$ and a challenge $\Omega \in_R \{g^{ab}, R\}$, it is hard to decide whether $\Omega = g^{ab}$ or $\Omega = R$.*

Assumption 2. *Let $g^{a_i}, g^{b_i}, i = 1,2,\ldots,t$ be given. Also let, $\Omega_1 = (l_1, l_2, \ldots, l_{t+1})$, $\Omega_2 = (l'_1, l'_2, \ldots, l'_{t+1})$, where $l_i = g^{a_i b_i} g^{m_i}$ and $l'_i = g^{a_i b_i} g^{n_i}, i = 1,2,\ldots,t$ and $l_{t+1} = \frac{1}{\prod_{j=1}^{t} g^{a_i b_i}} g^{m_{t+1}}, l'_{t+1} = \frac{1}{\prod_{j=1}^{t} g^{a_i b_i}} g^{n_{t+1}}$. Again assume, $g^{\sum_{i=1}^{t+1} m_i} \stackrel{c}{\approx} g^{\sum_{i=1}^{t+1} n_i}$. Now, given $\Omega \in \{\Omega_1, \Omega_2\}$, it is hard to decide whether $\Omega = \Omega_1$ or $\Omega = \Omega_2$.*

Lemma 5.2. *DDH assumption implies assumption 2.*

Proof. According to the DDH assumption given $g, g^{a_i}, g^{b_i}, g^{a_i b_i} \stackrel{c}{\approx} R$. Hence, $g^{a_i b_i} g^{m_i} \stackrel{c}{\approx} R \stackrel{c}{\approx} g^{a_i b_i} g^{n_i}, \forall i \in [t]$. Hence, $\Omega_1 = (l_1, l_2, \ldots, l_{t+1}) = (g^{a_1 b_1} g^{m_1}, g^{a_2 b_2} g^{m_2}, \ldots,$
$g^{a_t b_t} g^{m_t}, \frac{1}{\prod_{j=1}^{t} g^{a_i b_i}} g^{m_{t+1}}) \stackrel{c}{\approx} (g^{a_1 b_1} g^{m_1}, g^{a_2 b_2} g^{m_2}, \ldots, g^{a_t b_t} g^{m_t},$
$\frac{1}{\prod_{j=1}^{t} g^{a_i b_i} g^{m_i}} g^{\sum_{i=1}^{t+1} m_i})$
$\stackrel{c}{\approx} (R_1, R_2, \ldots, R_t, \frac{1}{\prod_{j=1}^{t} R_i} g^{\sum_{i=1}^{t+1} m_i}) \stackrel{c}{\approx} (R_1, R_2, \ldots, R_t, \frac{1}{\prod_{j=1}^{t} R_i} g^{\sum_{i=1}^{t+1} n_i})$
$\stackrel{c}{\approx} (g^{a_1 b_1} g^{n_1}, g^{a_2 b_2} g^{n_2}, \ldots, g^{a_t b_t} g^{n_t}, \frac{1}{\prod_{j=1}^{t} g^{a_i b_i} g^{n_i}} g^{\sum_{i=1}^{t+1} n_i})$
$\stackrel{c}{\approx} (g^{a_1 b_1} g^{n_1}, g^{a_2 b_2} g^{n_2}, \ldots, g^{a_t b_t} g^{n_t}, \frac{1}{\prod_{j=1}^{t} g^{a_i b_i}} g^{n_{t+1}})$
$= (l'_1, l'_2, \ldots, l'_{t+1}) = \Omega_2.$ □

Proof. Let us denote the compromised machines as $N_1, N_2, \ldots, N_\kappa$. The election authority chooses the critical parameters for all the compromised machines. This includes the scores and the secret keys. So, the adversary $\mathcal{A}$ can compute the ballots for all the compromised machines. Let us also assume that the secret key of N_i is $(x_{i1}, x_{i2}, \ldots, x_{in})$ and the corresponding public key is $(g^{x_{i1}}, g^{x_{i2}}, \ldots, g^{x_{in}})$. Hence the ballot of $N_i, i \in [k+1, n]$ will be $C_i = (c_{i1}, c_{i2}, \ldots, c_{in})$ when M is used as the matrix of local trust values. We again assume that the ballot of N_i is $C'_i = (c'_{i1}, c'_{i2}, \ldots, c'_{in})$ when M' is the matrix of local trust values. Here, $c_{ij} = g^{x_{ij} y_{ij}} g^{t_i v_{ij}}$ and $c'_{ij} = g^{x_{ij} y_{ij}} g^{t_i v'_{ij}}; \forall i, j \in [n]$. We know that $g^{x_{nj} y_{nj}} = \frac{1}{\prod_{k=1}^{n-1} g^{x_{kj} y_{kj}}}, \forall j \in [n]$. Hence, $c_{nj} = \frac{g^{t_n v_{nj}}}{K_j \prod_{k=\kappa+1}^{n-1} g^{x_{kj} y_{kj}}}$. According to the assumption $\sum_{i=k+1}^{n} t_i v_{ij} = \sum_{i=k+1}^{n} t_i v'_{ij}, \forall j \in [n]$. Now, from assumption 2, we can say $(c_{k+1j}, c_{k+2j}, \ldots, c_{nj} K_j) \stackrel{c}{\approx}$
$(g^{x_{k+1j} y_{k+1j}} g^{t_{k+1} v_{k+1j}}, g^{x_{k+2j} y_{k+2j}} g^{t_{k+2} v_{k+2j}},$
$\ldots, g^{x_{n-1j} y_{n-1j}} g^{t_{n-1} v_{n-1j}}, \frac{g^{t_n v_{nj}}}{\prod_{z=k+1}^{n} g^{x_{zj} y_{zj}}}) \stackrel{c}{\approx}$
$(g^{x_{k+1j} y_{k+1j}} g^{t_{k+1} v'_{k+1j}}, g^{x_{k+2j} y_{k+2j}} g^{t_{k+2} v'_{k+2j}},$
$\ldots, g^{x_{n-1j} y_{n-1j}} g^{t_{n-1} v'_{n-1j}}, \frac{t_n v'_{nj}}{\prod_{z=k+1}^{n} g^{x_{zj} y_{zj}}}) =$
$(c'_{k+1j}, c'_{k+2j}, \ldots, c'_{n-1j}, c'_{nj} * K_j)$. Hence the lemma holds. □

5.2 Privacy and Integrity Analysis

We analyze the privacy of collaborating machines in two aspects: first the adversary does not know the scores of the collaborating machines, and secondly, the scores on the bulletin board are unlikable. Each machine can have the global reputation of other machines from the public bulletin board, which could not be used in correlation with local information or information from other colluding machines to infer the local feedback values of the target machines and their relationship network (which machine are connected with other and exchange messages). The published feedback on the bulletin board is the valid score of either $-1, 0, or 1$ in the following format $g^{xy}g^{v}$ for $v = -1, 0, or 1$. The associated 1-out-of-3 NZKP reveals nothing more than the statement of feedback correctness: the v is either $-1, 0 or 1$. The encrypted feedback values ensure that participating users would not learn anything about the feedback expects final aggregated reputation score. The aggregation protocol is secure even if the number of feedback providers colludes with each other. The final global reputation is public on the public bulletin board, and it is impossible to ensure the privacy of feedback if exceptional all interacted machine of target machine collaborate with each other, but this is the extreme scenario. The feedback values are fully protected if adversary colludes with only a few interacted machines of the target machine.

6 CONCLUSION

In an M2M network, machines not only reports events from the physical world to the centralized analytic center for the meaningful decision but also provide value-added services to the end-users. These machines operate autonomously and do not require human interaction for monitoring, analytics, and services. The compromised or untrusted machines can be used to spread malicious content, can also report false information about the monitored environment, thus can have catastrophic consequences in certain scenarios. The development of secure, reliable and privacy preserving reputation system can be an effective solution to identify the untrusted and malicious machines in an autonomous Machine to Machine network in a timely and secure way. This paper described an M2M-REP system that enables machines or system administrators to securely compute the global trustworthiness of machines in a complete decentralized and privacy-preserving way. The proposed M2M-REP ensures that the machines or aggregator cannot learn anything about the participating machines other than the aggregated global reputation score which is not privacy sensitive. We presented the model for the two scenarios: a honest-but-curious model and the malicious model. The semi-honest model is more efficient in terms of computation and bandwidth requirement, whereas the malicious model is expensive but provide an effective defense against the presence of malicious machines. As a part of the future work, we are intended in developing the pro-type of proposed system and also incorporate the mechanism for personalized reputation aggregation.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their constructive comments. This work is supported by ERC Starting Grant No. 306994.

REFERENCES

[1] D. Evans, "The internet of things how the next evolution of the internet is changing everything," *White Paper Cisco Internet Business Solutions Group (IBSG)*, 2011.
[2] G. Intelligence, "Cellular m2m forecasts: unlocking growth cellular m2m connections forecast to reach 1 billion by 2020," 2015.
[3] B. TECH, "Fridge sends spam emails as attack hits smart gadgets," 2014.
[4] X. Lin, "Cat: Building couples to early detect node compromise attack in wireless sensor networks," in *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, Nov 2009, pp. 1–6.
[5] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266, May 2014.
[6] Z. Yan, W. Ding, V. Niemi, and A. V. Vasilakos, "Two schemes of privacy-preserving trust evaluation," *Future Generation Computer Systems*, vol. 62, pp. 175 – 189, 2016.
[7] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 53–59, April 2011.
[8] I. Stojmenovic, "Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 122–128, April 2014.
[9] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *2010 First IEEE International Conference on Smart Grid Communications*, Oct 2010, pp. 238–243.
[10] A. Narayanan and V. Shmatikov, "De-anonymizing social networks," in *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, ser. SP '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 173–187.
[11] M. Joye and B. Libert, *A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 111–125.
[12] A. Michalas and N. Komninos, "The lord of the sense: A privacy preserving reputation system for participatory sensing applications," in *2014 IEEE Symposium on Computers and Communications (ISCC)*, June 2014, pp. 1–6.
[13] E. Pavlov, J. S. Rosenschein, and Z. Topol, *Supporting Privacy in Decentralized Additive Reputation Systems.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 108–119.
[14] N. Rishab and R. Karthik, "Fuzzy privacy preserving peer-to-peer reputation management," *IACR Cryptology ePrint Archive*, 2009.
[15] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th International Conference on World Wide Web*, ser. WWW '03. New York, NY, USA: ACM, 2003, pp. 640–651.
[16] O. Hasan, L. Brunie, E. Bertino, and N. Shang, "A decentralized privacy preserving reputation protocol for the malicious adversarial model," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 949–962, June 2013.
[17] O. Hasan, L. Brunie, and E. Bertino, "Preserving privacy of feedback providers in decentralized reputation systems," *Comput. Secur.*, vol. 31, no. 7, pp. 816–826, Oct. 2012.
[18] S. Clauß, S. Schiffner, and F. Kerschbaum, "K-anonymous reputation," in *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '13. New York, NY, USA: ACM, 2013, pp. 359–368.
[19] F. Hao, P. Y. A. Ryan, and P. Zielinski, "Anonymous voting by two-round public discussion," *IET Information Security*, vol. 4, no. 2, pp. 62–67, June 2010.

APPENDIX

Key well-formedness

Here we show how a machine can generate a NIZK proof of knowledge of x_{ij} given $g^{x_{ij}}$. The prover generates a random $r \in_R \mathbb{Z}_p$ and computes a commitment $com = g^r$. Let, the challenge of the NIZK proof be ch. The prover calculates a response $res = r - ch * x_{ij}$. The prover publishes the commitment com and the response res. The verification equation is as follows:

$g^{res} \stackrel{?}{=} com/(g^{x_{ij}})^{ch}$. If this equation is satisfied, then the proof is correct. The NIZK proof has one commitment and one response. Hence, the size of the proof is 2. Computation of this proof requires 1 exponentiation and the verification requires two exponentiations.