Trust based Clustering Architecture for the Internet of Things

Oumaima Ben Abderrahim
National School of Computer Science
Tunis, Tunisia

Mouhamed Houcine Elhdhili
National School of Computer Science
Tunis, Tunisia

Leila Saidane
National School of Computer Science
Tunis, Tunisia

***Abstract*—The Internet of things is based on the idea that surrounding things of the human living space can be connected to the Internet. Adoption of the Iot cannot be approved unless security problems are resolved. Security solutions for the Iot can be built on special architectures as dividing a mobile network in clusters managed by a cluster head, called clustering. However, without any security considerations, the clustering process is prone to various security internal attacks. To protect the Iot against inside malicious nodes, a trust management system might be used as it has proved its security efficiency and friability in mobile network. In this paper we propose a trust based clustering algorithm for the Internet of Things**

Keywords— Internet of things; Clustering; trust management; Security

INTRODUCTION

The Iot was first proposed in 1998 [1] as an extension of the current Internet where objects can communicate directly or indirectly with electronic equipments that are connected to the Internet. Iot can be considered as a collection of independent systems that operate with their own infrastructures based, in part, on the existing infrastructure of the Internet. It covers three types of communications that can be established in restricted areas: from to person to object, from object to object and from machine to machine. Using multiple technologies such as RFID and sensor networks, objects will be located, identified, monitored and controlled remotely. This will form a universal and ubiquitous network that will support the development of intelligent and low consumption serving citizens cities. Moreover, the interconnection of physical objects with the Internet should increase the already significant network communications impact on society on a large scale, and thus, gradually lead a genuine paradigm shift [2]. The Iot architecture is usually divided into three layers [3], including perception layer (context aware tier), network layer, and application layer. The perceptual layer is the important layer which collects heterogeneous information through physical equipment like RFID Reader, GPS and sensors. The second level is the network layer which represents the core of the IoT. It integrates various wired and wireless networks to accurately transfer the information of things. It is responsible for the reliable transmission of information from the perceptual layer to the application layer. Finally, the application layer provides the personalized services according to users' needs such as accessing the IoT through the application layer interface by using a mobile. Security in this network should be included in all layers. However, this cannot be accomplished unless Iot security challenges are solved by designing new protocols adapted to Iot characteristics and constraints because security solutions used in Internet are not adapted for the Iot. Moreover, Iot involves heterogeneous objects belonging to various environments such as human surrounding things, sensor networks, mobile communications and the Internet. Thus, security solutions should take into accounts especially heterogeneity and privacy. The conventional security solutions such as cryptography and key management are effective against external attacks but they remain ineffective against internal attacks as malicious nodes in a network can act correctly in some times and incorrectly in other ones.. Thus, settling down a trust management system might be interesting to mitigate these malicious behaviors.

The rest of the paper is organized as follows: Section 2 deals with existing Iot trust management solutions presented in the literature. In section 3, we present trust based clustering architecture for the Iot. In section 4, we present our new trust management system based on the clustering architecture for IoT. Finally we conclude the paper and outline future works.

I. RELATED WORK

Trust is used in various contexts and has multiple meanings. Usually, trust mechanisms are employed by people in daily life to promote social relationships, friends, family, etc. According to Grandison and Sloman [4], trust management is defined as "the activity of collecting, codifying, analyzing and evaluating evidence relating to competence, honesty, security or dependability with the purpose of making assessments and decisions regarding trust relationships" Trust management has been deeply addressed in mobile networks for enforcing security and analyzing the behavior of nodes. CONFIDENT, proposed by buchelger and sulk [5], is

a popular distributed packets system for transmission services, the goal of this system is the detection of malignant nodes that can disrupt the operation of a network, and therefore allows to make a good decision in the future. The proposed system takes into account direct and indirect observations to update the value of trust. According to this model, direct observations are not always reliable in cases where the nodes of the network have constraints as interactions rare or frequent changes of requirements. So, indirect observations might supply nodes with a larger vision of the network leading to more accurate decisions. However, CONFIDENT assumes that only the negative feedback can be propagated in the network, recess the system with such a hypothesis is vulnerable to false report.

In [6] Michiardi and Molva propose the CORE model as a generic mechanism based on reputation to uphold cooperation between nodes in a MANET to prevent selfish behavior. Each network entity keeps track of other entities reputations. Reputation is computed on the basis of different types of information on the rate of the collaboration of each entity. The model assigns a global trust value to a cooperating node for all provided services. CORE assumes that only positive feedback can be propagated in to network. Thus, nodes have no interest to give false praise on uncertain nodes recess. However, the system with such a hypothesis is vulnerable to false positive evidences to increase their reputation values. RFSN, proposed by Ganeriwal and Srivastava in [7] is the first trust based model proposed for wireless sensor networks to monitor sensor nodes interactions. The value of the trust is calculated based on direct observation from watchdog mechanism and indirect observation from other nodes. RFSR assumes that only positive witnesses can be propagated to avoid bad mouthing based attacks. Works on trust management systems in the context of Internet is limited. In [8], chen et al have noticed that establishing trust relationships between heterogeneous entities is a complex task. They pointed out the related security risks and challenges and proposed security architecture for the Internet of things [9], according them the most objects are linked to human entities and are capable of establishing social relationships as friendship, ownership and community. However, malicious nodes can disturb the network functionalities using attacks as self-promoting, bad mouthing and good mouthing. In [9], authors propose a distributed trust management protocol for IoT. This protocol is based on encounter and activity rates: two nodes that come in touch to each other or involved in a mutual interaction can directly rate each other and exchange trust evaluation of other nodes, performing an indirect rate which seems to be like a recommendation. Three reference parameters for trust evaluation are used: honesty, cooperativeness, and community-interest. Therefore, such a dynamic trust management protocol is capable of adaptively adjusting the best trust parameter setting in response to dynamically changing environments in order to maximize application performance. SIOT is a similar approach proposed by Niti and

Al [11], it is a subjective model based on social relationships where each node computes the trust on the basis of its own experience and the opinion of common friends. In this system the weight of the transaction increases with the amount of the transaction, for the evaluation of trust, the authors uses a feedback system, Credibility and centrality of objects. In [12], authors proposed a trust management system based on fuzzy reputation for the IoT with QoS trust metrics containing elements as packets forwarding/delivery ratio and energy consumption. However, this system considers that the environment of the IoT is formed only sensors, which is far from satisfying the goal of the IoT services.

A. *Maintaining the Integrity of the Specifications*

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

II. TRUST BASED CLSUTERING ARCHITECTURE FOR THE INTERNET OF THINGS

In this section, we will propose a cluster based trust management system for the IoT. The network will be divided into clusters managed by cluster heads based on electing metrics including trust levels of nodes. Our primary goal is to reduce the likelihood of compromised or malicious nodes being selected (or elected) as cluster heads with the developing a trust-based framework for cluster-based internet of things.

A. *Assumptions*

We assume that our model is formed only by active object. Moreover, each object must be able to capture other objects, record their states, communicate with them and decides about their trust. We also assume that each object has a unique identifier.

B. *Metrics*

To decide which node can be elected as a cluster head, we consider the following metrics:

- *Trust level (T):* The cluster head will provide secure services in the network, that's why an object with a trust level less than a threshold "T-threshold" cannot be a candidate for being a cluster head even if it has high energy or low mobility.
- *Energy (E):* we must elect an object with high energy as a cluster head because it will ensure additional network and security functionalities as compared to ordinary nodes.
- *Connectivity (CO):* we must avoid choosing an object hidden or out of reach as the cluster head. To solve this problem, a node considered as a gateway periodically sends beacons. Only objects that receive these beacons may be candidates.

- *Stability (S):* It is better to elect the node with the nearest members as a cluster head. This might minimize node detachments and enhances clusters stability. Stability is computed as the cumulative mean square distance to neighbors divided by the total number of neighbors. The list of neighbors can be dynamically computed using hello messages while the distance to each neighbor can be estimated from the signal strength of a received hello messages.
- *Interest (I):* each object in our network shares an interest and provides only services related to its interest The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

C. Cluster formation

Iot is formed by heterogeneous and anonymous objects. However, cluster formation requires similarity between the participating objects. Thus, we propose a clustering algorithm based on the context and stability. Only objects that share common settings and are in well position can be a member of the same cluster. The grouped object based on similarity strengthens the security because members of a cluster will have a high rate of interactions. Besides, grouping the objects according to their positions or locations is very important because this will avoid detachment and loss of connections. It is assumed that the objects in the same cluster can reach agreement on trust because they share the same interests. We also assume that the communication between nodes and gateway is vulnerable to many attacks. Thus, we consider that only cluster heads can contact the gateway

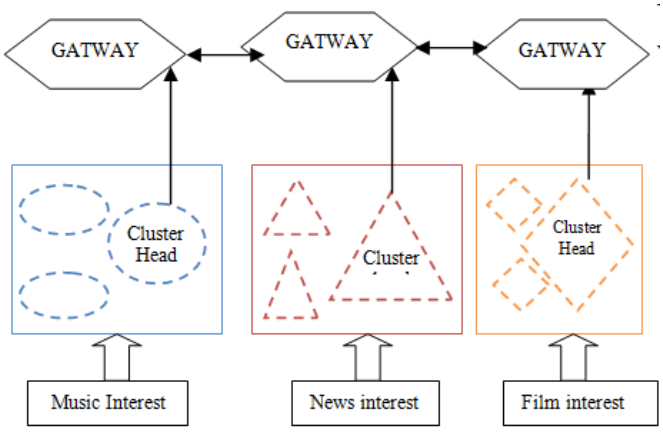

Fig1. Clustering architecture in Iot based on the context

D. Cluster head election protocol

The cluster head election protocol is defined as follows:
- Each object broadcasts a message containing the metrics (T, E, CO, S, I) as defined in the previous section
- Each node stores the metrics of its neighbors in a list L_m, determines the maximum of each metric and computes its weight as follows:

$T_m = T_i / T_{max}$
$E_m = E_i / E_{max}$
$CO_m = CO_i / CO_{max}$
$S_m = S_i / S_{max}$
$W_i = \alpha(1-T_{mi}) + \beta (1- E_{mi}) + \Omega C_{Omi} + £ I$ (1)
Where $\alpha+ \beta+ \Omega+£=1$

α, β, Ω, £ are used in the equation as weights for the metrics. Each object computes its W_i and compares it with the weights of other objects existing in L_m, if its weight is the minimum, it declares itself as cluster head by sending a Chmsg roles message to its neighbors. It launches a Dt timer to receive confirmation message by ordinary node Msg association to confirm their role as ordinary objects and their attachment to the cluster head.

In our algorithm we define 3 states:

- State 0 (*neutral member)* when an object has just arrived or it has just left its cluster and has not neighbors in its neighborhood, it state is not decided.
- State 1(Cluster *head):* The object has exchanged HELLO messages, and it has the lowest weight value. It creates a cluster in which it was appointed head of the cluster.
- State 2 (Cluster *member):* The object has exchanged HELLO messages; it has a low weight value compared to its symmetric neighbors, and is part of the cluster members.

We also defined 3 steps:

- Step 0: All objects are at the initial state (neutral), each object sends a hello message containing their metrics, each object determines the maximum metrics are then calculated weight. Then each object compares its weight with its neighbors
- Step 1: if it has the lowest compared to its neighbors, a node reaches state 2 (cluster head). Once in state 1, node i triggers a counter Cptr. If after passing this timeout, the node i hasn't received HELLO message that means it has any neighbors in its radio range, so it decides to move to state 0 (not decided state).
- Step 2 weight isn't minimum compared to neighbors weights, object goes to state 2 (cluster member). Once in state 1, node i triggers a counter Cptr. If after passing this timeout, the node i hasn't received a HELLO message that means it has any neighbors in its radio range, so it decides to move to state 0 (not decided state).
- Step 3 if the weight of cluster head exceeds the threshold, a new chief election mechanism is triggered, and then the cluster head reaches state 1.

E. Cluster member assignment protocol

After defining a cluster head election protocol, how a new object can decide which cluster to join? To solve this problem the cluster head broadcasts periodic discovery packets. Objects that receive these packets analyze data and may decide to join the cluster and attach to the cluster head by sending a request to join packet. The result should be

communicated to other cluster members (ordinary objects and cluster head)

F. Update algorithm

Each object sends periodic hello messages to the other cluster objects containing its metrics. Thus, the trust level is dynamically updated based on the direct and indirect observations. Each cluster head sends periodic unicast messages for ordinary and other cluster heads. After receiving this message, each object updates its cluster head list and neighbors trust values based on direct and indirect observations.

At any time an object in the network can decide to join or leave the network. To keep the network organization, the cluster head, before dismissing, must give the leadership role to another object. It chooses the object with minimal weight and sends to it an attachments message. When a cluster head dismisses improperly, it will be deleted from cluster head list and it will be considered as untrusted.

III. TRUST MANAGEMENT

In this section we will define how nodes trust levels is managed.

A. Assumptions

Usually, the value of the trust is presented between 0 and 1 as it is suggested by [13] and [14] or between -1 and 1 as it is described in [15], in our work we use the value of trust as a value between 0 and 1.

- It is assumed that if the trust value <0.5 the Object is malicious. If the value of the confidence = 0.5; the object is uncertain. If the value of the trust> 0.5, the object is trusted.
- It is assumed that objects in our network are divided into two categories: smart object and ordinary object. It is also assumed that smart objects have more power to launch attacks.

B. System parameters

The parameters used for the calculation of trust by our model are:

- *Feedback system (f*) "Assessment of the transaction" to evaluate the transaction "L", a node 1 requests a transaction L from Node B, and it expressed its satisfaction with 0 or 1.
- *Total number of transactions* (S): Total transactions between node A and B
- *Transacting factor* (Ω): to measure the weight of transaction L between two nodes A and B, this parameter increases with the amount of the transaction. Or nodes can be honest as unique services.
- computation capabilities *(C*), objects with large capacity such as smart phones are more likely to launch more attacks so we ought to assign a weight to each object based on its category

Object categories	weight
Smart Object	0.3
Ordinary Object	08

Table 1: computation capabilities

- Intensity*:* The intensity is denoted by $I_A(B)$ and represents the number of times that B has interacted with A

C. Trust computation steps

The calculation of the trust in our model takes tow topologies: intergroup topology where distributed trust management is used and intra-group trust or centralized management system. In the Intergroup topology, each object computes the value of the trust for all other group members based on direct and indirect observations. Then, each object sends the value of the trust to its neighborhood and to its cluster head. The trust policy basis is that two mobiles that are strangers to each other can still trust each other if they share enough common knowledge confidence. For the bootstrap problem, the user may force the creation of a historical element when trusts an object belonging to one of these trusted knowledge.

Phase bootstrap:

Initially, the history of an object is empty, the protocol cannot therefore function properly, a solution is considered a prior screening bootstrap phase in which the user is directly involved, which is the only one able to manually validate first confidence interaction, this phase aims to enrich the history analogous to the model Bluetooth (in this model, a single credential - PIN - must be manually entered on each mobile After generating a secret session key, the mobile can authenticate and encrypt their communications)

Trust computing on the node level:

Each object keeps a table of trust where it records all the trust levels of its neighbors for each service.

When two strangers meet each others for the first time, they exchange some or all (depending on their security policy) of their history entries (each element represents a node in whom they trust and with whom they have interacted). Then, they look for the number of trusted nodes that would be shared and according to their political trust; interaction can take place if the number is greater than a given threshold.

Let d_T is timing window is used to measure the number of transaction successes and failures, it consists of several units of time, the interactions that occur in each time unit within the timing windows are saved. If the transaction is success the feedback = 1 else the feedback = 0. Objects in IoT provide different services from different major, so it is associated with each transaction a weight W, the value of W increases with significant transaction.

As we already mentioned, the network is formed by objects with different capacity, powerful objects such as smart objects have more ability to cheat against other objects that's why it is assigned weight for each class of objects. After interaction the value of trust will update, the intensity is increased and the date of the last interaction is updated

Let S is the number of successful transaction (feedback = 1), the calculation of the trust in our algorithm as follows

$T_{ij}= (1-\alpha)\ T_{ij}\ (t- \chi t) + \alpha T_{ij}$

$T_{ij} = \lambda O^{direct} + \beta O^{Ind} + \alpha I_{ij} + \gamma C_j$

$O^{direct} = \frac{\sum_1^{In} S1 * wij^l}{wij^l}$

$O^{ind} = \frac{\sum_1^{Irec} S1 * wij^l}{wij^l}$

D. Scability

The Internet of Things is a network characterized by scalability, so at a certain moment, the memory of each cluster member will be saturated. Our algorithm computes the rate of interaction which is the average number of applications services performed by a node per unit time knowing that the time unit is defined by our protocol. We assume that each object remains at rest without communication duration higher than the threshold will be automatically deleted from the trust table of cluster member.

E. Analysis and discussion

Clustering is a popular technique that is used to organize the systems characterized by scalability, but this technique is ineffective if it is not protected against attacks, in our article, we applied a clustering architecture for our network based on the interest and trust; it was assumed that only the objects that share a common interest can communicate. We classified the objects into two categories, smart objects and ordinary objects with giving to each object a weight. In our architecture, only the CH, the most powerful and trustworthiness object can communicate with the getaway. This is a strong point for the security of our network since the getaway is exposed to attacks. After the calculation of the trust, each objects recorded in a table of Trustworthiness the value of the trust for each transaction with different metrics as indicated in the table below.

Nodes	Category	Transaction	Metrics	Trust
Node i	Smart object	L1	….	….
Node j	….	L2	…..	…
Node …	…..	….	….	….

Table 2: Table of trust

Then each object sends the value of trust to the chef cluster, the later will save the value of trust.

CONCLUSION

In this paper, we have presented a clustering based trust management protocol for the Internet of things. The cluster head is the powerful and stable objet which ensures secure communication between the objects. Our solution can increase the lifetime of our network and protect the network against attacks by reducing the likelihood of the election of Compromised or malicious nodes as cluster heads. As future work we will prove the performance of our approach to ensuring the security of our network against attacks and increasing the life of our network experimentally through simulations. We will improve our approach by securing the communication between the objects and between object and gateways.

REFERENCES

[1] R. H. Weber, “Internet of things – new security and privacy challenges,”Computer Law & Security Review, vol. 26, pp. 23-30, 2010J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73

[2] The EPC global Architecture Framework. EPC global Final Version 1.3, Approved 19 March, 2009. http://www.epcglobalinc.org

[3] Zhuankun Wu. : Initial Study on IOT Security architecture. J. Strategy and decision-making research (2010)

[4] T. Grandison and M. Sloman. Specifying and analysing trust for internet applications. In Proceedings of the Second IFIP Conference on e-Commerce, e-Business and e-Government, 2002

[5] Buchegger S, Boudec J-YL. Performance analysis of the CONFIDANT protocol. In: Proc. 3rd ACM int. symp. mobile ad hoc netw. comput., Lausanne, Switzerland 2002. p. 226e36.

[6] Michiardi P, Molva R. CORE: a COllaborative REputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Proc. 6th int. conf. commun. Multimedia security 2002. p. 107e21.

[7] Ganeriwal S, Srivastava MB. Reputation-based framework for high integrity sensor networks. In: Proc. ACM security for adhoc and sensor networks 2004. p. 66e7

[8] Chen D, Chang G, Sun D, Li J, Jia J, Wang X. TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things. Comput Sci Inf Syst Oct. 2011;8(4):1207e28

[9] Bao F, Chen IR. Dynamic trust management for Internet of Things Applications. In: 2012 International workshop on self-aware Internet of Things, San Jose, California, USA September 2012

[10] Michele Nitti, Roberto Girau. A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things. 23rd Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications

[11] Chen D, Chang G, Sun D, Li J, Jia J, Wang X. TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things. Comput Sci Inf Syst Oct. 2011;8(4):1207e28

[12] Y.L. Sun, W. Yu, Z. Han, and K.J.R. Liu, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks,” IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006

[13] G. Theodorakopoulos and J.S. Baras, “On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks,” IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 318-328, Feb. 2006

[14] A.A. Pirzada and C. McDonald, “Establishing Trust in Pure Ad-Hoc Networks,” Proc. 27th Australasian Computer Science Conf. (ACSC ’04), pp. 47-54, Jan. 2004.