A Similarity based Trust Model to Mitigate Badmouthing Attacks in Internet of Things (IoT)

Vijender Busi Reddy*, Atul Negi†, S Venkataraman‡ and V Raghu Venkataraman§
* ‡ §Advanced Data Processing Research Institute (ADRIN)
Department of Space, Govt. of India
Secunderabad, India
* †School of Computer and Information sciences
University of Hyderabad
Hyderabad, India
Email:*vijender@adrin.res.in,†atulnegi@uohyd.ac.in,‡kalka@adrin.res.in,§director@adrin.res.in

***Abstract*—In Internet of Things (IoT) each object is addressable, trackable and accessible on the Internet. To be useful, objects in IoT co-operate and exchange information. IoT networks are open, anonymous, dynamic in nature so, a malicious object may enter into the network and disrupt the network. Trust models have been proposed to identify malicious objects and to improve the reliability of the network. Recommendations in trust computation are the basis of trust models. Due to this, trust models are vulnerable to bad mouthing and collusion attacks. In this paper, we propose a similarity model to mitigate badmouthing and collusion attacks and show that proposed method efficiently removes the impact of malicious recommendations in trust computation.**

***Index terms*—** IoT, Trust, Recommendations, Similarity, Privacy.

I. Introduction

Semantically IoT is "A world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [1]. IoT is a evolving paradigm in the modern wireless communication scenario. The objects or Things in IoT could be RFID (Radio-Frequency Identification) devices, sensors, smart phones etc. These objects interact mutually and exchange data. Each object is identifiable remotely and sufficiently intelligent for its data communication and processing requirements. It is well known that objects and users connected to the Internet are extremely vulnerable. Attackers exploit the fundamental weakness of the network to disrupt the services. In Smart Cities environment, Things may be in remote or not be attended for long time.

For IoT to be widely accepted as reliable many challenging issues need to be addressed [1]. This paper concentrates on security and reliability issues of IoT. Most of IoT objects are mobile and use wireless communications which makes IoT objects vulnerable to several attacks e.g., "eaves dropping", "black hole" attacks, "DoS" attacks, "packet modifications" attacks, "replay" attacks, etc. IoT objects work by cooperation with neighbouring objects for transmitting required information to any intended destination. Trust management plays a crucial role in IoT for reliable data transfer, data security, information reliability, services etc. Malicious objects greatly degrade the performance of IoT [2]. Trust based security solutions [3] were proposed to identify malicious objects in IoT networks. These solutions not only provide security but also give confidence to objects on neighbors for interaction. Objects in IoT networks evaluate neighbouring objects and based on this evaluation, decide the engagement and interaction. Objects may share information about their trust on neighbouring objects as recommendations.

978-1-5386-4980-0/19/$31.00 2019 IEEE

Recommendation trust models aggregate recommendations received from neighbours. A malicious node may send false recommendations so that legitimate nodes get low trust values. This is called as a bad mouthing attack [4]. Sometimes malicious nodes collude with each other and send bad recommendations on a particular target node, called as a collusion attack. Recommendations must be weighed based on the credibility of the recommender, to mitigate these kind of attacks. In literature [5, 6], authors use direct trust as credibility but the main problem with this approach is that a node may appear to work sincerely but it may send false recommendations. Similarity mechanisms allow to correlate recommendations so as to compute credibility of a node. In this paper, we propose a similarity mechanism to compute the credibility of a node.

The remaining part of this paper is organized as follows. Section 2 briefly explains the recent trust mechanisms. Section 3 provides the proposed trust mechanism and simulation results are presented in section 4. Finally we conclude paper in section 5.

II. Related Work

Before going into recent trust models we first explain certain basic concepts of trust. Trust is an individual belief and it quantifies the relationship between two nodes to maintain reliable communication [6]. Trust can be measured as a continuous value [0,1] where 0 is distrust and 1 is fully trustable. Discrete values [-1,0,1] can also be used to measure trust where -1 is distrust, 1 is fully trustable and 0 is neither trust nor distrust. Threshold based approaches use a threshold value to identify the node's trustability [6].

Objects compute trust about their immediate neighbouring objects. Any object computes trust based upon their own expe-

rience called as direct trust. Objects also receive recommendations from neighbouring nodes about any particular node. These recommendations are used to compute indirect trust. Some malicious objects may send wrong recommendations which leads to inconsistency in trust computation.

Now we describe some of the popular trust models in Adhoc networks. CORE [7] uses watchdog mechanism to calculate the trust. CORE exchanges only positive recommendations which restricts propagation of malicious nature of a mobile node. Another approach CONFIDENT [8] uses both direct and indirect recommendations to calculate trust, and uses ALARM messages to identify the malicious nodes. SORI [9] uses direct observation and recommendation based mechanisms to compute trust. SORI drops packets based upon a probability computed on the trust value of a node. Both these approaches use direct trust as a credibility parameter. An object may appear to behave well but send wrong recommendations.

TWSN [10] use similarity mechanism to compute the credibility of a recommender. Authors use Root Mean Square (RMS) based model to correlate the recommendations with their own experience. Several surveys have been done on trust computation mechanisms in Ad-Hoc wireless Networks [11, 12, 13, 14].

Al-Hamadi et. al. [15] proposed a trust based decision making system for health IoT systems. Authors used three parameters such as risk classification, reliability and loss of health probability for building the trust. This trust value is used to assess the reliability of a IoT device as well as health loss of the patient. This trust model computes the parameter based on query/response of the IoT device.

Yuan et. al. [16] proposed a trust mechanism for IoT edge devices. Feedback trust from a broker is used to compute Feedback trust. Overall trust is computed based on direct trust between device to device and Feedback trust from broker. Feed back trust correctness depends on broker's credibility.

In this work, we propose a recommendation trust model for IoT networks which uses a similarity model to suppress wrong recommendations.

III. Proposed approach

The main aim of this paper is to provide an effective trust mechanism for IoT. We assume that all objects have similar capabilities. Here, badmouthing and collusion attacks are addressed. We first define the parameters used for the proposed trust computation.

A. Direct Trust

Direct trust is computed based on a node's own experience in the neighbourhood. Observations on packet forwarding behaviour is used to compute direct trust. Algorithm 1 computes direct trust ($Direct\_Trust$) values based on a node's packet forwarding behaviour. *packet_sent* function returns *TRUE* if node sent packets. *packet_forward* function returns *TRUE* if node detects promiscuously a packet forwarded by neighbouring node.

Algorithm 1 Direct trust computation algorithm

procedure DIRECTTRUST
  packets_sent $\leftarrow 0$
  packets_forwarded $\leftarrow 0$
loop:
  if *packet_sent(j) == TRUE* **then**
    $packets\_sent \leftarrow packets\_sent + 1.$
  if *packet_forward(j) == TRUE* **then**
    $packets\_forwarded \leftarrow packets\_forwarded + 1.$
$Direct\_Trust[j] = packets\_forwarded/packets\_sent$
goto *loop*.
close;

B. Recommendation Credibility

Nodes receive recommendations from neighbouring nodes. Some malicious neighbours may send wrong or false recommendations. To identify these false recommendations recommendation credibility is required. Recommendation credibility represents the node's capability to provide correct recommendations. A novel similarity mechanism is proposed to identify such false recommendations. Recommendation credibility is used to reduce the impact of false recommendations in indirect trust computation.

A and *B* are two nodes and N_{AB} denotes the set of common neighbours to A and B. $|N_{AB}|$ is the cardinality. The recommendation credibility ($Recom\_credibility$) is computed based on Algorithm 2. δ is the threshold parameter for similarity verification.

Algorithm 2 Recommendation credibility computation algorithm

procedure RECOMMENDATION CREDIBILITY
  //Direct_TrustA and Direct_TrustB arrays are
  $//received from neighbouring nodes A and B$
  diff $\leftarrow 0$
  sim_count $\leftarrow 0$
  for $i \leftarrow 1$ *to* $|N\_AB|$:
  $diff \leftarrow diff + [Direct\_TrustA - Direct\_TrustB]^2$
  if $(Direct\_TrustA - Direct\_trustB) < \delta$ **then**
    $sim\_count \leftarrow sim\_count + 1$
$D \leftarrow sqrt(diff/|N\_AB|)$
$Recom\_credibility \leftarrow (1 - D) \times (sim\_count/|N_{AB}|)$
close;

C. Indirect Trust

Indirect trust is computed by aggregating the recommendations sent by neighbouring nodes on a particular node. Here, we use weighted average mechanism where weight is the *Recommendation credibility*.

Indirect trust ($Indirect\_Trust$) is computed based on Algorithm 3.

Algorithm 3 Indirect trust computation algorithm

procedure INDIRECT TRUST
  //N is the total number of neighbours
  numerator $\leftarrow 0$
  denaminator $\leftarrow 0$
  for $i \leftarrow 1$ *to* N :
  $numerator \leftarrow numerator + [Recom\_credibility[i] * Direct\_trust[i]]$
  $denominator \leftarrow denominator + Recom\_credibility[i]$
$IndirectTrust \leftarrow numerator/denominator$
close;

Parameter	value
Simulation Time	*600 sec*
Number of nodes	*25*
Area	*1200×900*
Transmission Range	*150m*
Transport protocol	*UDP*
Application protocol	*CBR*
Radio interfaces	*4*

TABLE I
SIMULATION PARAMETERS

D. Node Trust

Node Trust is the weighted mean of direct and indirect trust values. $NodeTrust$ is node's trust value computed as follows:

$$NodeTrust = \alpha \times Direct\_Trust + (1-\alpha) \times Indirect\_Trust \quad (1)$$

where α is weight of the direct trust which is decided based on the application.

IV. SIMULATION RESULTS

We evaluate the proposed method in presence of malicious nodes. We have integrated the proposed model with Ad-hoc On-demand Distance Vector (AODV) [4] routing protocol in *ns-2* [17]. 26 nodes are randomly deployed in an area of $600 \times 600\, m^2$. Malicious nodes are placed randomly in the network. The experiments are done in presence of 15% malicious nodes which performs packet dropping, badmouthing and collusion attacks. The results are taken in presence of badmouthing and collusion attacks. Simulation parameters are given in Table 1.

The recommendation credibility parameter is evaluated with some popular similarity measures [18] those are: Pearson correlation, Cosine correlation and Root Mean Square similarity. The objective of this experiment is to show the effectiveness of the proposed recommendation credibility parameter with other similarity models.

Similarity models are computed on six different data sets. In all cases the proposed method performed well. Fig. 1 shows Pearson, cosine similarity, RMS similarity and proposed recommendation credibility values of six example data sets. *proposed1* is computed based on algorithm 2 with *sim_count* is *1* if both sets show similar neighbour behavior otherwise the value is *0*. *proposed2* is computed based on algorithm 2 with *sim_count* is *1* if both sets show good and similar neighbour behavior otherwise the value is *0*.

DATA-I		DATA-II		DATA-III	
X	*Y*	*X*	*Y*	*X*	*Y*
0.860000	0.900000	0.960000	0.910000	0.960000	0.910000
0.840000	0.970000	0.410000	0.230000	0.410000	0.230000
0.930000	0.820000	0.360000	0.490000	0.360000	0.490000
0.930000	0.880000	0.970000	0.880000	0.370000	0.280000
0.910000	0.910000	0.940000	0.790000	0.140000	0.790000
0.980000	0.950000	0.980000	0.770000	0.980000	0.770000
0.880000	0.970000	0.980000	0.970000	0.980000	0.970000
pearson= -0.315071		pearson= 0.912019		pearson= 0.616550	
cosine= 0.996437		cosine= 0.991033		cosine= 0.920898	
RMS_sim = 0.922448		RMS_sim = 0.865517		RMS_sim = 0.725722	
proposed1 = 0.922448		proposed1 = 0.865517		proposed1 = 0.544291	
proposed2 = 0.922448		proposed2 = 0.618226		proposed2 = 0.311024	
DATA-IV		**DATA- V**		**DATA-VI**	
X	*Y*	*X*	*Y*	*X*	*Y*
0.600000	0.900000	0.950000	0.910000	0.790000	0.100000
0.890000	0.670000	0.950000	0.930000	0.890000	0.100000
0.470000	0.820000	0.960000	0.890000	0.910000	0.100000
0.930000	0.480000	0.970000	0.100000	0.960000	0.100000
0.960000	0.910000	0.940000	0.100000	0.940000	0.100000
0.940000	0.100000	0.980000	0.100000	0.780000	0.100000
0.780000	0.100000	0.980000	0.100000	0.980000	0.100000
pearson= -0.378584		pearson= 0.485954		pearson= Inf	
cosine= 0.805443		cosine= 0.739484		cosine= 0.996618	
RMS_sim = 0.516870		RMS_sim = 0.343364		RMS_sim = 0.203732	
proposed1 = 0.221516		proposed1 = 0.147156		proposed1 = 0.000000	
proposed2 = 0.221516		proposed2 = 0.147156		proposed2 = 0.000000	

Fig. 1. Pearson, cosine correlation, RMS similarity and proposed similarity method(R_A^B) values of example data sets

Even though X and Y sets are appearing to be with similar values in DATA-I (in Fig. 1), Pearson shows a lower similarity score. The data sets X and Y are independent to each other, Pearson does not give an accurate similarity. DATA-II (in Fig. 1) shows cosine similarity is high. Pearson is not useful on DATA-VI (in Fig. 1) because Y set has repeated values. Cosine similarity shows highest similarity in all the cases. RMS similarity (*RMS_sim*) is low when more number of values are not similar. It is observed that no similarity mechanism works perfectly on all kinds of data. The proposed method shows better similarity score for all six types of data sets. It is shown that the proposed recommendation credibility i.e., proposed2 is more accurate in computing similarity value between two nodes.

Fig. 2 and 3 show the recommendation credibility value of legitimate and malicious nodes. The objective of this experiment is to show the recommendation credibility value of a legitimate and malicious node in presence of badmouthing and collusion attacks. We computed the recommendation credibility value in two scenarios of badmouthing attacks.

a. Fig. 2 shows the recommendation credibility of a legitimate and a malicious node. Here, malicious node send recommendations as 0.1 for every legitimate node.

b. Fig. 3 shows the recommendation credibility values as complement of its actual trust value i.e $(1 - actual\, trust\, value)$. In both scenarios proposed method accurately computing the recommendation credibility value.

In both cases the recommendation credibility of a malicious node is low and legitimate node's recommendation credibility

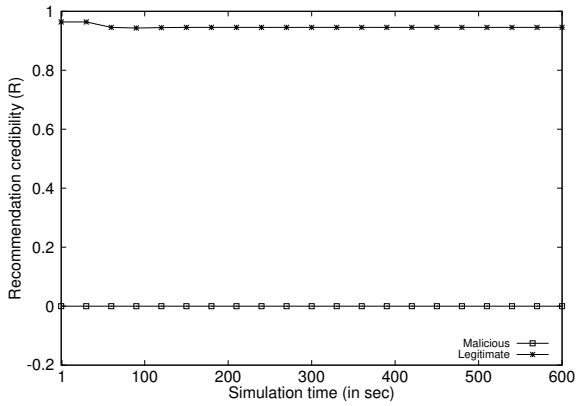

Fig. 2. Recommendation trust computation by proposed model with constant bad recommendation

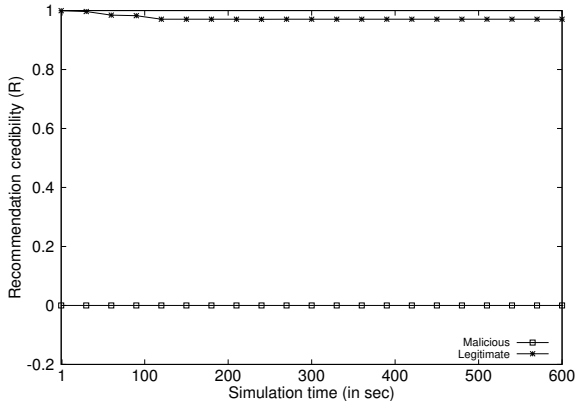

Fig. 3. Recommendation trust computation by proposed model with dynamic bad recommendation

is high. The proposed recommendation credibility is effectively computing the weight. Weight being low implies the recommendation of that node has lower contribution in indirect trust computation.

Fig. 4 shows recommendation credibility against number of bad recommendations. As % of bad recommendations increases, recommendation credibility decreases. The contribution of recommendations are reduced based on the correct recommendations received from that neighbour.

V. Experimental Evaluation

We have experimented the proposed algorithm by deploying the nodes with UHF modems and sensors as shown in Fig. 5. We use location sensors for sending the location information to cloud. Nodes are Android phones with HC12 modules [19] connected through mini USB port. Each node is connected to its neighbour through UHF modem (HC12 module). HC12 module has radio range upto 100 meters. Here, the sensors collect information and send it to nodes. Nodes send these information to cloud for further processing. Some nodes have mobile data connection to send information to cloud. Proposed algorithm is implemented to assess forwarding behaviour of

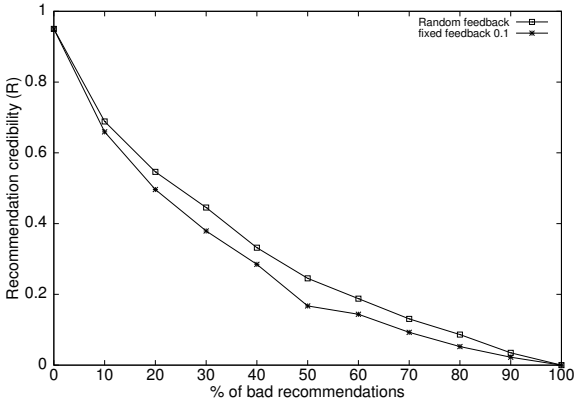

Fig. 4. Recommendation trust computation by proposed model with % of bad recommendations

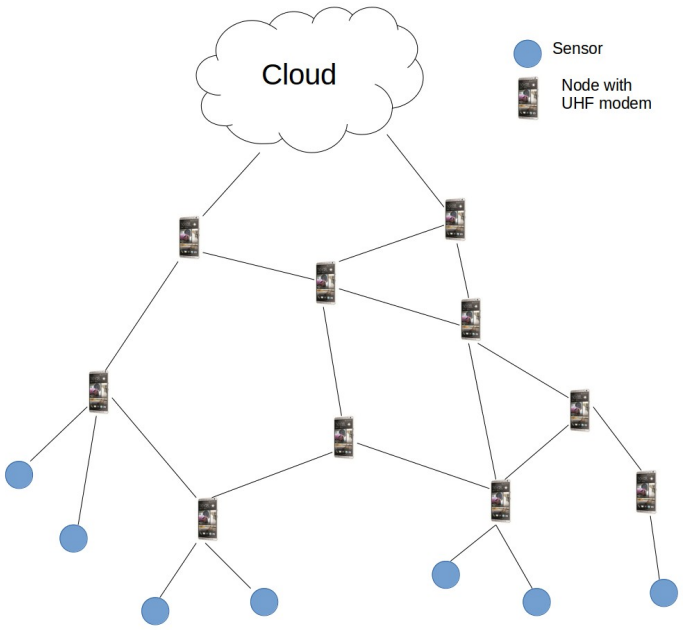

Fig. 5. Experiment model

the nodes. We have deployed three malicious nodes in the network. Routing algorithm with trust value is implemented same as in [20]. Sensors send information periodically (10 seconds) to Cloud.

We experimented the proposed method in two conditions. i.e. constant bad recommendations and dynamic bad recommendations. In both cases the number packets received from sensors are higher compare to the nodes without trust model. Sensors generate 2520 messages every one hour. With trust model is implemented the cloud receive 2417 messages from different sensors. Whereas 1824 messages are received by cloud without trust model implementation. So, the information received by cloud is less in presence of malicious nodes. Proposed method successfully identify the malicious nodes and omits these nodes from routing path gives more packet

delivery to cloud which leads to improvement in decision making.

VI. Conclusion

We have proposed a trust model for IoT to mitigate packet dropping, badmouthing and collusion attacks. Instead of using direct trust as weight in computing the indirect trust we propose a novel similarity model to compute the recommendation credibility. This recommendation credibility is used as a weight in indirect trust computation to reduce the impact of false recommendations in trust computation. We have evaluated the performance of the proposed model in presence of malicious nodes and shown that it is effective in computing the true set of trust values. Therefore we conclude that our proposed similarity mechanism can be used to identify malicious recommendations instead of direct trust as recommendation credibility. In future, we plan to implement the proposed model on physical devices and perform experiments.

References

[1] G. M. Luigi Atzori, Antino Iera, "The internet of things: A survey," *Elsevier journal on Computer Netwroks*, vol. 54, pp. 2787–2805, 2010.

[2] A. V. V. Zheng Yan, Peng Zhang, "A survey on trust management for internet of things," *Elsevier Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.

[3] A. S. J.-H. Cho and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 13 Issue 4, pp. 562–583, 2011.

[4] C. S. R. Murthy and B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*. Prentice Hall, 2004.

[5] M. M. I. Anupam Das, "Securedtrust: A dynamic trust computation model for secured communication in multiagent systems," *IEEE Transactions on Dependable and Secure Computing*, vol. Vol. 9, No. 2, pp. 261–274, March/April 2012.

[6] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 14 issue 2, pp. 279–298, 2012.

[7] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *6th Int. Conf. Commun. Multimedia Security*, Pp107-121, 2002.

[8] S. Buchegger and J. L. Boudec, "Performance analysis of the confidant protocol," in *3rd ACM International Symposium Mobile Ad Hoc Networks, Lausanne, Switzerland*, 2002.

[9] D. W. Q. He and P. Khosla, "Sori: A secure and objective reputation based incentive scheme for ad-hoc networks," in *IEEE Wireless Communications and Networking Conference*, 21-25 March 2004.

[10] S. V. Vijender Busi Reddy and A. Negi, "Communication and data trust for wireless sensor networks using ds theory," *IEEE Sensors Journal*, vol. 17, no. 12, pp. 3921–3929, 2017.

[11] R. I. A. Josang and C. Boyd, "A survey of trust and reputation systems for online service provision," *Elsevier journal on Decision support systems*, vol. 43, no. 2, pp. 618–644, 2007.

[12] H. C. C. Fan Hsun Tseng, Li Der Chou, "A survey of black hole attacks in wireless mobile ad hoc networks," *A Springer open access journal on Human Centric computing and Information sciences*, pp. 1–16, 2011.

[13] C. M. C. L. H. Yu, Z. Shen and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *IEEE Proceedings*, vol. 98 Issue 10, pp. 1755–1772, 2010.

[14] J. Zhang, "A survey on trust management for vanets," in *2011 IEEE International Conference on Advanced Information Networking and Applications, Singapore*, 2011, pp. 105–112.

[15] I. R. C. H. Al-Hamadi, "Trust-based decision making for health iot systems," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1408–1419, 2017.

[16] X. J. Yuan, "A reliable and lightweight trust computing mechanism for iot edge devices based on multi-source feedback information fusion," *IEEE Access*, vol. 6, pp. 23 626–23 638, 2018.

[17] N. simulator 2, ""http://www.isi.edu/ns"."

[18] Y. S. Keunho Choi, "A new similarity function for selecting neighbors for each target item in collaborative filtering," *Elsevier Knowledge-Based Systems*, vol. 37, pp. 146–153, 2013.

[19] R. Rozee. (2016, January) Hc-12 wireless serial port communication module v2.3, "https://www.elecrow.com/433mhz-serial-rf-module-hc12-1000m-p-874.html". [Online]. Available: https://www.elecrow.com/433mhz-serial-rf-module-hc12-1000m-p-874.html

[20] A. N. Vijender Busi Reddy and S. Venkataraman, "A dynamic trust evolution model for ad hoc networks based on mobility," *International Journal of Ad Hoc and Ubiquitous Computing Journal (IJAHUC)*, vol. 28, Issue 4, pp. 230–246, 2018.