International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys.13, No.1 (May-23)

http://dx.doi.org/10.12785/ijcds/130195

DTM-CPS: Dynamic Trust Management Mechanism for Cyber Physical System based on Dirichlet Reputation System

Kanchana Devi V[1], Karmel A[1], Umamaheswari E[1], Kiruthika S[2], David Maxim Gururaj A[1] and Nebojsa Bacanin[3]

[1]*Vellore Institute of Technology, Chennai, Tamilnadu, India*
[2]*Government Polytechnic College, Vanavasi, Salem, Tamilnadu, India*
[3]*Singidunum University, Belgrade, Serbia*

Received 6 Apr. 2022, Revised 4 May. 2023, Accepted 14 May. 2023, Published 30 May. 2023

Abstract: In Cyber Physical System (CPS), data protection is considered as an important factor when sensors are employed in hostile environment. The sensors are highly prone for security threats like compromised nodes, who's crypto keys embedded in the security chip are physically captured by adversaries easily. Compromised node attack are launched by the attackers by physically capturing the cryptographic keys in remote region and becoming the internal node. Traditional protection mechanisms are mostly based on cryptography, which failed to address this kind of threat. Trust Management Mechanism based on rating, ranking, weight schemes help in building a secure, flexible and available system and provides second level of security for such compromised node attack. This paper presents a dynamic trust management mechanism for Cyber Physical System based on Dirichlet Reputation System (DTM-CPS). The simulation result shows that, this DTM-CPS has a better performance and security for CPS than traditional trust management mechanisms.

Keywords: Compromised Node Attack, Cyber Physical System, Dirichlet Reputation System, Network Security, Trust Management System

1. INTRODUCTION

With the emergence of Cyber Physical System (CPS), the development of respective standards and technology, CPS security demands higher challenges. Firstly, the security threats of the CPS are analysed with security demands, several studies come up with variety of ideas in the research work of the CPS security related problems, and study the required technologies, system, and several industrialization issues of the CPS security. Secondly, system applications security of CPS is considered based on the industry is endorsed, means, the security mechanisms inside the industry is resolved by itself. The uniquely designed specifications adhere to traditional industry directives. The general contemplation of CPS is its open security for users, components, and assigned different level of security [1][2]. Along with information association of the CPS and by enhancing the pertinent information decrease security uncertainty in CPS.Traditional Internet has already carried a series of deliberations on such security issues. CPS system demands special review in the security. This is because of the reality that, data integrity and data authenticity are not assured, then the reliability of the processing behind big data and cloud computing is unsophisticated. CPS is a dynamic environment, which consists of both static and dynamic networks. The dynamic network has a requirement for a systematic and effectual communication among nodes. In traditional approaches in such wireless networks view static or dynamic nodes [3].

Using CPS, the communication among nodes obtain ample of information in Cyber Systems, and perceive a cooperative interaction in physical systems. CPS is usually defined as the integration of the cyber system and the physical system [4]. CPS is composed of wireless and independent nodes and these nodes instantly form a wireless network without a prior defined infrastructure. Generally, the security threats in CPS are come from security attacks. These type of security attacks are categorised as exterior and interior attacks. Encryption, decryption, digital signature and authentication in [5] are some methods which defend against exterior attacks. But the specified techniques failed to address the interior attacks. In this case, the security mechanisms are added up with trust management in order to address the interior attacks. Another, security and trust problems related to CPS are existing. The latent spoofing, denial-of-service (DoS), impersonation, and eavesdropping attacks decreases the cyber systems nodes trust, and it causes the safety, performance and efficiency issues on the physical systems [6]. Traditional trust mechanisms fail to

E-mail address: kanchanadevi@vit.ac.in, karmel.a@vit.ac.in, umamaheswari.e@vit.ac.in, kiruthikavishnu@live.com, davidmaxim.gururaj@vit.ac.in

address these issues with the demand of dynamic interactions between nodes. Since, these interactions triggers the unwanted traffic.

The main goal of this paper is to design a futuristic dynamic trust management mechanism to describe the logical association among nodes or the devices in the network. The designed trust model resists against various malicious attacks both exterior and interior along with deceptions based on the assessment and certificate-based mechanisms. Moreover, the proposed trust architecture decreases the communication overhead among the nodes.

Section 2 describes about the review on literature. Section 3 represents the detailed description Dirichlet-Distribution with Reputation Calculation. Section 4 provides Research Contributionwith complete explanation on DTM-CPS: Dynamic Trust Management Mechanism for CPS based on Dirichlet-Distribution. The experimental result and the analysis on simulation is presented in Section 5. Finally, Section 6 presents a short discussion and conclusion on the work done.

2. LITERATURE REVIEW

In this section, we discuss and examine the trust management mechanisms which are based on various probability distributions such as Dirichlet distribution, Beta distribution, and Gaussian distribution, and later, the technical specifications of these distributions are described. Generally, the reputation model in trust management mechanisms uses a probabilistic model or the statistical model for trust calculations, among these techniques the Beta distribution [7] is most commonly used probabilistic distribution for trust, and then in some schemes the Gaussian distribution is embedded [8].

A. Trust Models: Dirichlet Distribution

Kanchana Devi et. al., in [9] has presented a trust based selfish node detection method using beta distribution. Here, monitoring the environment happens with the help of sensor nodes using Watchdog Mechanism (WDM). Selective Forwarding and continuous dropping of packets which are to be forwarded to the next adjacent node are major issues which seeks the attention of researchers in order to build a highly secure network. The compromised nodes become the internal attackers and launches several attacks like selective dropping of packets. These problems are addressed by the authors in the proposed model by identifying selective dropping of packets and continuous dropping of packets by incorporating Beta probabilistic distribution. Rani et al., in [10] proposed a malicious node detection mechanism using Dirichlet Distribution in trust model for WSN. The malicious nodes perform certain attacks such as damaging communication among the nodes leads to the packet loss, decreases forwarding packets and devise unstable data communication. This model provides security solution which resist ballot and bad-mouthing attacks for WSN. This model generates a trust evaluation with trinomial Dirichlet distribution. It combines the gathered evidences are combined using both standard deviation rule and Dirichlet fusion rule. This model includes sliding methodology and penalty for malicious nodes. The experimental results of this model show improvement compared to existing trust models mainly to detect malicious attacks and packet delivery ratio is increased in wireless sensor networks. Fung et. al. [11] presents CIDN: Collaborative Intrusion Detection Network, shows the intrusion detection accuracy depends completely on the efficient collaboration among the peers. A Dirichlet distribution-based trust management is used to measure the trust level among intrusion detection depends on their interaction experience. An algorithm called acquaintance management is used to allow all intruders mainly to manage its familiarity on their truthfulness. This approach promotes scalability and robustness against interior attacks. This provides efficiency in CIDN. This model is evaluated by formal simulation, it demonstrates its scalability, robustness, and the efficiency with existing models.

In [12][13] a DTMS-IoT: Dirichlet based trust management system for the IoT and DDTMS has been designed to detect malicious nodes. This model minimizes dynamic on-off attack and wrong recommendation attack. In [14]Traditional trust models use direct observations and recommendations for computing trust. This paper proposes two major solutions. The first solution purely based on node recommendations. The second solution resist dynamic on-off attack with the help of history factor and minimizes wrong recommendations. This is achieved by using K-means algorithm. The experimental results show that this DTMS-IoT stood up against the common on-off and ballot-stuffing attack. Li et al., [15] has implemented DDOA: A Dirichlet-Based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System. In this paper, the compromised local agents are identified with Dirichlet distribution mainly to reduce financial frauds in electricity prices. A reputation-based trust is established between the local agents in smart grid. An incentive mechanism enabled algorithm is used to quickly identify the attackers. For experimentation, IEEE 39-bus power system data is used in power world simulator. Hang et al.,[16] has designed a framework reputation computing for wireless sensor network. This framework has structured in two aspects i. Detection ii. Reputation. The detection aspect uses LOF outlier algorithm for identifying the outliers. Secondly, in reputation calculation Dirichlet distribution is implemented to calculate belief and uncertainty level. Here the behaviour of each node is observed and the observed information is recommended for the other nodes. The simulation results present that the faulty nodes are easily identified and the proposed model has been compared with framework with beta probability distribution.

B. Trust Models: Beta Distribution

Fang et. al., [17] has proposed BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks. This model determines the compromised nodes which causes severe internal attacks. This model uses beta

probability to model the values captured by monitoring the node behaviour. The beta probability distribution produces a trust value which is later used for choosing relay nodes and to minimize the internal attacks caused by compromised nodes. The model computations are implemented in a simulator and verifies that this model resist all sort of compromised nodes with energy level and trust data. Ganeriwal et. al., [18] investigated data accuracy in Wireless Sensor Network with a generalized method. This method supports trust among community nodes. For achieving this, a framework is developed with reputation calculation based on past and present behaviour of the nodes and future behaviour of the node is predicted. The authors used Beta Reputation System which is based on Bayesian formula. In motes this framework act as the middleware. The correctness of this framework is tested based on Mica2 motes – lab-scale Test, simulation-Avrora and in James Reserve with real-time data set. This framework mainly aims at sensor node data integrity and accuracy.

Wu et. al., [19] has designed a trust mechanism for Wireless Sensor Network to address the behaviour based trust calculation. The authors investigated Beta Distribution and Link Quality Indicator. In this model, three types of trust are devised such as (i) Trust for Communication (ii) Trust for Energy (iii) Trust for Data. The weight for each of the trust is computed based on the beta distribution. Later, an algorithm is proposed for assessing the quality of the link and alerts the corresponding node. The experiments are conducted based on certain parameters such as stability of the network and the accuracy of the network. This model withstands against various attacks caused internally when compared to other traditional mechanisms. Ahmed et. al., [20] has designed a WPTE: Weight based Probabilistic Trust Evaluation method. It purely depends on Beta Probability for modelling the trust of node. This model identifies the faulty nodes and misbehaving nodes in the network and extends the lifetime of the network. It ensures the reliable data delivery. This model is compared with other trust models with the parameters like cost of communication, convergence of trust and trustfulness degree. This WPTE provides robustness in less communication cost with high trust convergence. This model is highly recommended for WSN which works in hostile environment. Uma et al. [21] has developed an enhanced beta trust model to address the problems such as energy consumption, packet loss and to reduce the time taken to reach the sink node in wireless sensor network. This model discovers the malicious nodes which causes the above said problem. By identifying these malicious nodes, improvises the throughput of the corresponding network. The problem causing malicious nodes are called as insiders according to the author. Mahmud et. al., [22] introduces a Brain-Inspired Trust Management Model for Neuroscience application which is based on IoT framework. This paper use behavioural and data trust for calculating adaptive neuro fuzzy inference system along with weighted additive method. The traditional fuzzy based trust models show that the accuracy and robustness for detection of malicious nodes. Compared to traditional trust models, this proposed model provides strong security mechanism to ensure reliable and secure connection between end node. Yin et. al., in [8] investigated a penalty-based trust model for Wireless Sensor Network. This model completely relies on Beta Probability mathematical distribution. Delay in on/off attack is the main cause of malicious attack. In this model, the redemption-based penalty method is used for calculating trust value. Authors have simulated the same using the MATLAB environment. The simulation results show that, this model increases the sensitivity against detecting malicious attacks. Momani et. al., [23] has extended their previous work by presenting trust component based on communication and data which is misled by the network. Using Bayesian distribution, a greater number of trust components are combined to generate the overall trust. The authors prove that, the proposed model is general and robust which suits all sort of Wireless Sensor Network.

C. Trust Models: Gaussian Distribution

Gaussian is a type of continuous probability distribution. Sinha et. al., in [24][25] has developed a Gaussian trust-based framework with reputation combination for MIMO-WSN. It incorporates the indirect information from the communication made between the nodes. This framework uses expert opinion based on Bayesian method for reputation calculation. Also, a multivariate novelty model is proposed based on Gaussian mathematical distribution. A framework for reputation model based on time and trust aware HGPR: Heteroscedastic Gaussian Process Regression has been designed. In which, the framework gathers the input and produces a reputation-based feedback similar to WSN in [26]. This model targets the web services trust through the interaction reputation is calculated.

3. Introduction on Dirichlet-Distribution with Reputation Calculation

This Dirichlet Distribution is one among the continuous multivariate probabilistic distribution with the parameter represented using a vector. This Dirichlet distribution is used with prior distribution rely on Bayesian Statistics. Typically, probability distribution of several occurrences which are positive are independently repeated n number of times in Bernoulli experiment is caked the "binomial distribution" [27]. A common expansion of the before said binomial distribution is described as joint-probabilistic distribution of each variable. Assume $T = (t_1, t_2, \dot{.}..t_k)$, where, tiis represented as the probability of the Bernoulli's experimental output is type i and $t_i[0, 1]$. The variable i is usually limited between 1 and k, where $i = 1, 2, 3, \ldots, k$. The Dirichlet probabilistic distribution for t is represented as in Equation (1).

$$\rho(x|y) = \prod_{i=1}^{k} \gamma_i x_i \tag{1}$$

Where, $\gamma = \gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_k$ and $\sum_{i=1}^{k} \gamma_i = 1$. For the total of N sessions, the specified equation is represented as

$\sum_{i=1}^{k} \gamma_i = N$. Here, the conjugate prior distribution holds both the polynomial and Dirichlet probability distribution and the above expression becomes like in Equation (2)

$$\rho(\gamma|\alpha) = \alpha \prod_{i=1}^{k} \gamma_i \alpha_{i-1} \tag{2}$$

The PDF - Probability Density Function of Dirichlet Distribution after normalizing the Equation (2) is given in Equation (3).

$$Dirichlet(\gamma|\alpha) = \frac{1}{B(\alpha)} \prod_{i=1}^{k} \gamma_i \alpha_i - 1 \tag{3}$$

This Dirichlet probabilistic distribution is represented using Beta function, with applied normalization constant. Also, k type result with observation sequence is given below in Equation (4).

$$B(\alpha) = \frac{\prod_{k}^{i=1} \lambda(a_i)}{\lambda(\sum_{i=1}^{k} a_i)} \tag{4}$$

The parameter $x_i + \alpha_i$, are used in Dirichlet posterior distribution and given in Equation (5).

$$Dirichlet(\gamma x + \alpha) = \frac{1}{B(x + \alpha)} \prod_{i=1}^{k} \gamma_i^{(x_i + \alpha_{i-1})} \tag{5}$$

Assuming, $\alpha_i = 1(1)$, the Dirichlet probability Distribution with the probability $_i$ is given in Equation (6).

$$E(\gamma_i) = \frac{\alpha_i}{\sum_{j=1}^{k} \alpha_j} \tag{6}$$

The occurrences of relative probability are given by the above specified equations of I type sequences of events. With this, Equation (3) becomes as given below in Equation (7).

$$E(\gamma_i) = \frac{t_{i+1}}{n + \sum_{j=1}^{k} \alpha_j} \tag{7}$$

Beta probability distribution usually works with two parameters. In trust management mechanisms or systems, these parameters are used for counting or categorizing the events both positive and negative way. At the same time, Dirichlet probability distribution focuses more on communication behaviour among the nodes in the network. These observations are used for calculating the reputation of each node and also later, it is used for trust purpose.

A. *First-Hand Communication: Reputation Value Calculation*

In Dirichlet probability Distribution, three different parameters are used for reputation value calculations. Here, the three parameters are mapped with successful packet delivery, failure in packet delivery, and uncertainty in packet delivery. These three parameters are identified based on the communications takes place between the nodes in the dynamic network of CPS [28]. Unlike Beta distribution, this Dirichlet probability Distribution gives more importance for the uncertain behaviour of nodes in CPS network [29]. Since, Beta probability gives importance only for two main parameters called the success and failure. Here, $DX_{i,j}$ is used for the representation of trust value obtained by the first-hand communication between node iand node j. Also, the parameters $< S_{ij}, f_{ij}, u_{ij} >$ are used for various observations such as successful transfer of packet (S_{ij}), failure in packet transfer (f_{ij})and uncertainty in transfer of packet (u_{ij}). The history factor also has been given importance while calculating the reputation using first-hand communication. It is represented using ($\gamma_{history}$). The Dirichlet probability with the mapped parameters is given below in Equation (8).

$$DX_{(i,j)} = \frac{\delta_s S_{ij+1} \times (1 - \gamma_{history})}{\delta_s S_{ij} + \delta_f f_{ij} +_u u_{ij} + 3} \tag{8}$$

Each parameter is given different weightage for differentiating the behaviour while calculating the reputation value of node in CPS network. The weights for various behaviour are represented using $< \delta_s, \delta_f, \delta_u >$. Separately, the history factor is calculated using the Equation (9).

$$\gamma_{history} = \frac{\sum_{k=1}^{n} (f_{ij})_k - \sum_{k=1}^{n-1} (f_{ij})_k}{s_{ij} + f_{ij} + u_{ij}} \tag{9}$$

B. *Second-Hand Communication: Reputation Value Calculation*

Second-Hand communication plays a major role while building the reputation value of a particular node in the network. This second-hand communication is considered to be a double-edged sword. Since, with this second-hand communication information, the network becomes highly scalable and reputation calculation becomes easier. But, at the same time, untrusted nodes launch a newcomer attack to bring in the compromised nodes into the CPS network [30]. This splits the network into several disjoint network by inducing the compromised nodes to drop the forwarding packets. Some CPS network develops clusters for calculating the trust value in order to secure the entire network. In such cases, the trust values are calculated by the cluster nodes and summarized at the header node. The cluster head becomes the decision maker and categorizes the trusted and untrusted node in the network and later isolate them in the communication process. The steps involved in trust calculation by the second-hand communication is follows

- Nodes in the network are initialized with neutral trust value. Every communication or the interaction among the nodes are observed for the reputation calculation.
- The reputation values are calculated with the behavior of each node in the CPS network. A counter is maintained at each node. Here, if the packet is successfully delivered then the success counter gets incremented.
- Suppose, if the packet is not delivered the failure

counter maintained at the sender node gets incremented. Otherwise, the uncertainty counter gets incremented.

- These counter values are used for each trust value calculation by applying the Dirichlet Probability Distribution for each session for making decision whether the node involved in the communication can be trusted or not.
- This process continues for all the nodes as well as for all the sessions takes place during the complete communication.

The combined first-hand communication and second-hand communication are used for calculating one's reputation using the following Equation (10)

$$\begin{aligned} X_{ij} &= \alpha \times DX_{ij} + \beta \times RX_j \\ &= \alpha \times \frac{(\delta_s s_{ij} + 1)(1 - \gamma_{history})}{\delta_s s_{ij} + \delta_f f_{ij} + \delta_u u_{ij} + 3)} + \beta \times \frac{1}{N} \sum_{k=1, k\neq i, k\neq j}^{N} DX_{kj} \\ &= \frac{\alpha(\delta_s s_{ij+1})(1 - \gamma_{history})}{\delta_s s_{ij} + \delta_f f_{ij} + \delta_u u_{ij} + 3} + \frac{\beta}{N} \sum_{k=1, k\neq i, k\neq j}^{N} DX_{kj} \end{aligned} \tag{10}$$

Here, both α and β are considered to be the weights assigned for first-hand and second-hand communication respectively, and both these parameters need to satisfy the condition $\alpha + \beta = 1$. In the above section 3, the introduction to Dirichlet Probability Distribution and reputation value calculation by both the first-hand and second-hand communication has been explained. In the following section, the complete description of DTM-CPS has been provided along with detailed flow diagram of DTM-CPS has been given.

4. DTM-CPS: DYNAMIC TRUST MANAGEMENT MECHANISM FOR CPS BASED ON DIRICHLET-DISTRIBUTION

A. *Design of DTM-CPS*

In this section, the Dynamic Trust Management Mechanism for CPS based on Dirichlet Distribution (DTM-CPS) is designed. Firstly, the communication among the nodes are modelled on the basis of prior and posterior probabilistic distribution, which is known as "conjugate prior". Here, reputation is derived from node to node communication, which is modelled using Dirichlet Distribution. Communication among the nodes are usually defined as first-hand communication and second-hand communication. Depending on these, the reputation value varies. The communication history also plays a major role while modelling the reputation value using Dirichlet Distribution. With this gathered reputation value using first-hand and second-hand communication the trust value of each node is modelled with the Dirichlet Distribution. This computed trust value helps in deciding whether the node can be trusted or not with the help of threshold value. This trust value is allowed to exchange among the nodes in order to build the trusted network in a quicker manner. At the same time, this second-hand trust value exchange may lead to build a weaker network along with compromised nodes and network becomes irreparable for a longer period. This may breach the security of the whole network and becomes disjoint in lesser time. On the other hand, the scalability of the network becomes an easier task when it comes to second-hand communication. The network grows exponentially with this second-hand communication. The flow diagram of DTM-CPS is playing an exceptional task in endorsing trust calculation. The flow diagram of DTM-CPS is shown in Figure 1 In this flow diagram, three node networks are represented. The node observation has been categorized as (i) Normal Behaviour (ii) Abnormal Behaviour. These behaviour observations are used for reputation calculation using the Dirichlet Probability Distribution as specified in Section 3. All the observations are stored in order to be used for calculating the trust value. With these reputation value, the communicating node all the way detects the compromised nodes. These calculated reputation values are shared among the other nodes in the network called the "Second-hand Communication". These trust values are combined and update among all the nodes in the network. This particular process helps in building the trust and also the network becomes scalable. The calculated reputation values are used for making decision such as whether the node can be trusted or not.

5. SIMULATION AND EXPERIMENTAL ANALYSIS

The compromised node attack is launched by attacker for tossing packet dropping while communication takes place. In lower layer, by enabling promiscuous mode, one node can monitor the adjacent node's transmission. Since, it is applied in lower layer, it supports heterogeneous network. All the nodes in the network are initialized with 0.5 as trust value. The observation has been extended up to 200 packets during communication. In the simulation, nearly 2% of nodes are made malicious and it starts launching the packet dropping at the time of 80th and 160th packet communication. The three well known trust models are compared while calculating the trust value with the specified parameters and the results are shown in the below in comparison graph. In Figure 2, the comparison of trust value of three trust models are shown. Here, at the 80th slot the malicious node is activated and a slight drop is seen in the graph which represents drop in the trust value. Also, there is certain level of drop in trust value where the DTM-CPS resist against the compromised nodes in the network. Differences in the trust model are described in the below table. The trust value calculation among the nodes using DTM-CPS is captured and presented in the below Figures 3 and 4. Where, Figure 3 represents the trust value stability in normal circumstances. Also, the threshold value to differentiate the trusted node and untrusted node is provided as 0.5. Initially, every node is initiated with 0.5 as trust value in order to represent that every node in the CPS network is trusted. If the node maintains the trust value

TABLE I. COMPARATIVE STUDY OF VARIOUS TRUST MODEL WITH REGULAR AND ABNORMAL BEHAVIOUR

Trust Models/Status	Regular Behaviour	Abnormal Behaviour
GTM: Gaussian Trust Model	Trust value change is not observed in the communication process.	There is a drop observed while introducing the malicious node. Here, recovery process is less compared to Beta Probability Distribution.
BTM: Beta Trust Model	This Beta Trust Model holds the trust value which is the highest when compared with all the three distributions	Trust value decreases faster in Gaussian Distribution and the trust value is higher than DTM-CPS. Here, recovery process of trust values is quite faster compared with DTM-CPS.
DTM-CPS	Certain Jitter is observed in the trust value. Compared with the other two trust models this DTM-CPS shows better performance.	Trust value decreases faster than the other two trust models, and the minimum value of the trust value is observed here in this model and importantly, recovery process is better compared with the other two.

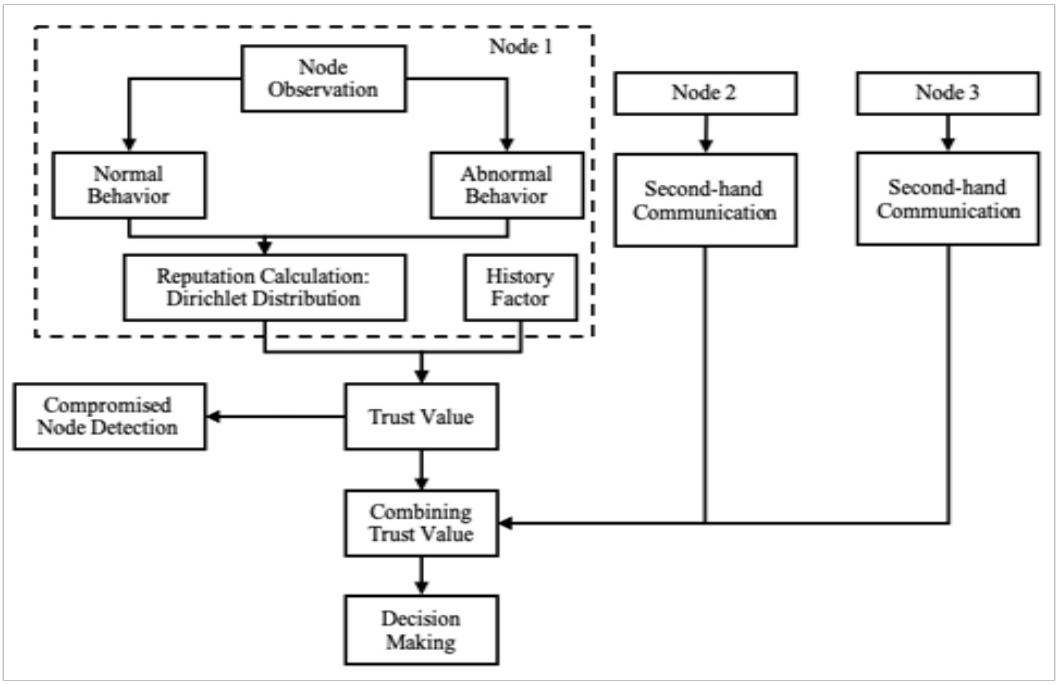

Figure 1. DTM-CPS: Flow Diagram

more than 0.5 then that node is categorized as trusted node and further communication of packets takes place with that node. Otherwise, that node is categorized as untrusted node and no more packets are transmitted to it. This scenario is represented in Figure 4. That is communication among the compromised node is captured and is shown in Figure 4.

As per the analysis, Dirichlet distribution-based trust management mechanism is comparatively superior than the other distribution mechanisms, and it simulates the node communication in a better way, considering supportive behaviour, non-supportive behaviour, and uncertainty. In the same way, this model maintains a maximum value that is comparatively more but not completely trusted node in CPS. In abnormal communication, the attack role is identified as soon as possible and efficiently by DTM-CPS. The succeeding pretending process of the misbehaving node does not help in increasing the trust value. Additionally, the DTM-CPS is customized according to the type of node communication to find the demands of heterogeneous

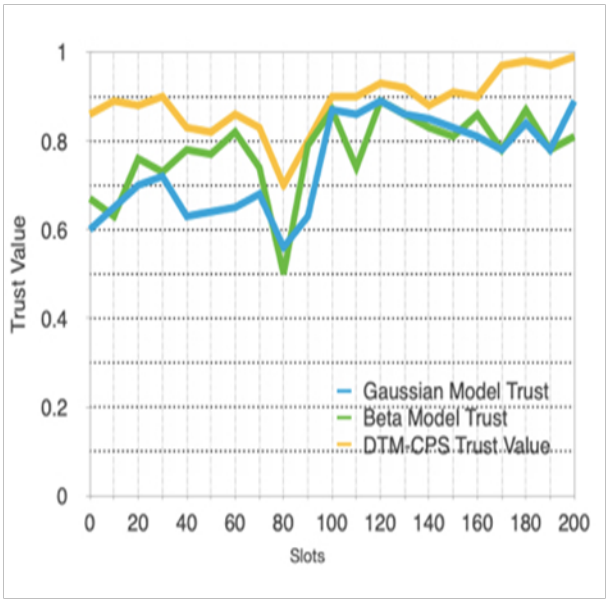

Figure 2. Gaussian, Beta and DTM-CPS Trust Value Comparison Chart

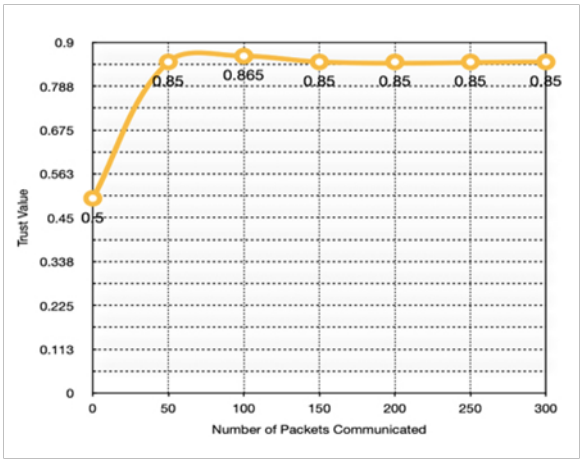

Figure 3. Changes in Trust Value - Normal Communication

network.

6. CONCLUSION OF THE WORK DONE

This paper discusses more about various trust management model such as Beta probability distribution, Gaussian distribution, and Dirichlet probability Distribution in a detailed manner. Here, the Dirichlet probability distribution uses node communication for reputation value calculation purpose. The first-hand and second-hand communication are used for the trust value calculation of each node in the CPS network. Along with the trust value, the compromised and malicious nodes are also identified. With the experimentation result, the proposed DTM-CPS has been proved to be best method in accurate identification of compromised nodes and calculates the trust faster among

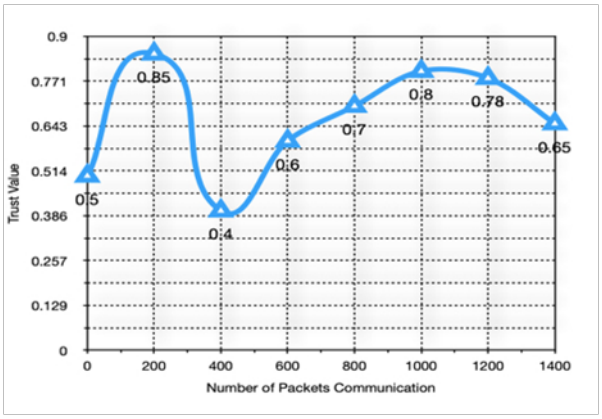

Figure 4. Changes in Trust Value - Malicious Node Communication

the other existing trust management models.

7. CONFLICTS OF INTEREST

This is to declare that, the manuscript has not been submitted to any other journal and is not under consideration elsewhere, none of the manuscript's contents has been previously published in any other journal, and the authors are aware of this submission and have no conflict of interest.

REFERENCES

[1] A. A. Khalil, J. Franco, I. Parvez, A. S. Uluagac, and M. A. Rahman, "A literature review on blockchain-enabled security and operation of cyber-physical systems," *CoRR*, vol. abs/2107.07916, 2021. [Online]. Available: https://arxiv.org/abs/2107.07916

[2] G. Hatzivasilis, I. Papaefstathiou, and C. Manifavas, "SCOTRES: Secure routing for IoT and CPS," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2129–2141, dec 2017. [Online]. Available: https://doi.org/10.1109%2Fjiot.2017.2752801

[3] B. C. S. P. Stehel, V. and S. Bilan, "Cyber-physical system-based real-time monitoring, industrial big data analytics, and smart factory performance in sustainable manufacturing internet of things," *Economics, Management, and Financial Markets*, vol. 16, no. 1, p. 42–51, 2021.

[4] Y. Liu, A. Liu, X. Liu, and M. Ma, "A trust-based active detection for cyber-physical security in industrial environments," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6593–6603, 2019.

[5] Q. Xu, Z. Su, and Q. Yang, "Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1098–1110, 2020.

[6] T. Ali, B. Marc, B. Omar, K. Soulaimane, and S. Larbi, "Exploring destination's negative e-reputation using aspect based sentiment analysis approach: Case of marrakech destination on tripadvisor," *Tourism Management Perspectives*, vol. 40, p. 100892, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2211973621001057

[7] Y. Y. Y. L. Weidong Fang, Wuxiong Zhang and W. Chen, "A resilient trust management scheme for defending against reputation time-varying attacks based on beta distribution." *Science China Information Sciences volume*, vol. 60, no. 040305, 2017.

[8] A.-S. Yin and S.-Y. Zhang, "A survey of trusted network trust evaluation methods," in *Security and Privacy in New Computing Environments*, J. Li, Z. Liu, and H. Peng, Eds. Cham: Springer International Publishing, 2019, pp. 87–95.

[9] K. Devi and R. Ganesan, "Trust-based selfish node detection mechanism using beta distribution in wireless sensor network," *Journal of ICT Research and Applications*, 2019.

[10] V. U. Rani and K. S. Sundaram, "Dirichlet distribution based trust model for malicious node detection in wireless sensor network," *Journal of Engineering and Applied Sciences*, vol. 14, pp. 4191–4199, 2019.

[11] C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Transactions on Network and Service Management*, vol. 8, no. 2, pp. 79–91, 2011.

[12] O. Ben Abderrahim, M. H. Elhedhili, and L. Saidane, "Dtms-iot: A dirichlet-based trust management system mitigating on-off attacks and dishonest recommendations for the internet of things," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, 2016, pp. 1–8.

[13] W. Fang, W. Zhang, L. Shan, X. Ji, and G. Jia, "Ddtms: Dirichlet-distribution-based trust management scheme in internet of things," *Electronics*, vol. 8, no. 7, 2019. [Online]. Available: https://www.mdpi.com/2079-9292/8/7/744

[14] C. Xu, J. Wang, L. Zhu, C. Zhang, and K. Sharif, "Ppmr: A privacy-preserving online medical service recommendation scheme in ehealthcare system," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5665–5673, 2019.

[15] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "Ddoa: A dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2415–2425, 2016.

[16] Q. Huang and H. NAN, "Reputation computing for wireless sensor networks based on dirichlet distribution," *Chinese Journal of Sensors and Actuators*, vol. 22, no. 4, pp. 11–14, 2009.

[17] W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, "Btres: Beta-based trust and reputation evaluation system for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 59, pp. 88–94, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S108480451500140X

[18] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sen. Netw.*, vol. 4, no. 3, jun 2008. [Online]. Available: https://doi.org/10.1145/1362542.1362546

[19] X. Wu, J. Huang, J. Ling, and L. Shu, "Bltm: Beta and lqi based trust model for wireless sensor networks," *IEEE Access*, vol. 7, pp. 43 679–43 690, 2019.

[20] A. Ahmed and A. R. Bhangwar, "Wpte: Weight-based probabilistic trust evaluation scheme for wsn," in *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 2017, pp. 108–113.

[21] V. UmaRani, K. S. Sundaram, and D. Jayashree, "Enhanced beta trust model in wireless sensor networks," in *2016 International Conference on Information Communication and Embedded Systems (ICICES)*, 2016, pp. 1–5.

[22] M. M. R. M. A. R. A. S. S. A.-M. . A. H. Mufti Mahmud, M. Shamim Kaiser, "A brain-inspired trust management model to assure security in a cloud based iot framework for neuroscience applications," *Cognitive Computation*, vol. 10, p. 864–873, 2018.

[23] M. Momani, S. Challa, and R. Alhmouz, "Bnwsn: Bayesian network trust model for wireless sensor networks," in *2008 Mosharaka International Conference on Communications, Computers and Applications*, 2008, pp. 110–115.

[24] R. K. Sinha and A. K. Jagannatham, "Gaussian trust and reputation for fading mimo wireless sensor networks," in *2014 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 2014, pp. 1–6.

[25] S. I. Singh and S. K. Sinha, "A framework for reputation model based on time and trust aware heteroscedastic gaussian process," in *2015 International Symposium on Advanced Computing and Communication (ISACC)*, 2015, pp. 16–20.

[26] J. Zhao, J. Huang, and N. Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks," *IEEE Access*, vol. 7, pp. 33 859–33 869, 2019.

[27] Y. Xiao, C. Lin, Y. Jiang, X. Chu, and X. Shen, "Reputation-based qos provisioning in cloud computing via dirichlet multinomial model," in *2010 IEEE International Conference on Communications*, 2010, pp. 1–5.

[28] D. Z. W. H. I. Eric Ke Wang, Chien-Ming Chen and K. L. Yung, "A dynamic trust model in internet of things," *Soft Computing*, vol. 24, p. 5773–5782, 2020.

[29] M. Mehdi, N. Bouguila, and J. Bentahar, "Trust and reputation of web services through qos correlation lens," *IEEE Transactions on Services Computing*, vol. 9, no. 6, pp. 968–981, 2016.

[30] Y. Guisheng, Z. Jianguo, and Y. Tongbao, "Study on the penalty function based on redemption mechanism for trust value of wsn," in *2012 6th International Conference on New Trends in Information Science, Service Science and Data Mining (ISSDM2012)*, 2012, pp. 683–688.

Kanchana Devi V is a Distinguished Professor in Vellore Institute of Technology, Chennai Campus, Tamilnadu, India. In March 2006, she received her Bachelor Degree in Computer Science and Engineering (College Topper), Mount Zion College of Engineering and Technology, Tamilnadu, India. In May 2009, She received her Master Degree in Computer and Communication (Gold Medal - Anna University) in Sri Sairam College of Engineering, Tamilnadu, India. In October 2019, She received her Ph. D in Computer Science and Engineering, Vellore Institute of Technology, Chennai Campus, Tamilnadu, India. Her research interests include Wireless Sensor Networks, Internet of Things, Cyber Physical Systems, Distributed Computing. Filed 2 Indian Patents, Received Funded Project from DST-DDP.

Karmel A is an Associate professor Grade - I, School of Computer Science and Engineering, VIT University, Chennai. She completed her B. E from MS university, M.E & PhD from Anna University, 2016. Her research area includes, Mobile Adhoc Networks, Network Security, IoT and Cyber Security. She had published around 25 research papers in SCI, Scopus indexed journals. She had received a project grant from DST. She is a Star Cyber Secure User-R11. She is an active ACM member. She had received best faculty award. She is a reviewer in reputed journals like Wireless Network, Mobile Network and Applications. She had published around 10 patents in the IPR Chennai. She had received research grant from Department of Science and Technology in the Device and Development Program. She had received research awards for her research projects, journal papers and patents.

E.UMAMAHESWARI is an Associate professor Grade II, School of Computing Science and Engineering, VIT University, Chennai. Currently she is associated with the Centre for Cyber Physical Systems. She completed her PhD in Anna University, 2015. Her area of specialization includes, Software Engineering (Testing, Metrics), Cloud Security, ERP, Machine Learning, Network Security, IoT. She had published more than 50 papers in SCI, Elsevier, Springer indexed journals. She is guiding more number of research scholars in the said specialization. She is an active ACM member and IEEE member. She is a gold medallist and a star performer in her master of science. She received best faculty award in the year 2008-2009. She is an editor for many journals in IGI global, Wiley publications etc., She is the reviewer in many journals to name a few Mobile Network and Applications. She was a PhD and Poster Track Chair in ICBCC from 2016 onwards, ICRTAC from 2019 onwards. She is the reviewer in Journal of Software, Future generation of computer system, MONET, wireless network, IGI global. She is also an editor of International Journal of web portal. She had published around 15 patents in the IPR Chennai. She had received research grant from Department of Science and Technology in the Device and Development Program. She had received research awards for her research projects, journal papers and patents.

Dr. S. Kiruthika is working as a Lecturer in Government Polytechnic College, Vanavasi, Salem. She worked as an Assistant Professor in the Department of ComputerScience and Engineering at Sona Collegeof Technology. She has completed herPhDin Information and Communication Engineering at Anna University in 2016, andhas a decade of experience in Teachingand Research. Her Research interests includeNatural Language Processing, Data Science,Business Analytics and Internet of Things.

Dr. David Maximum Gururaj A is working as Associate Professor in the School of Advanced Sciences. He has completed his PhD in Bharathiyar University, and has a decade of experience in Teaching and Research. His Research interests include Fluid Dynamics, published many papers in Scopus Indexed Journals. He had published around 3 patents in the IPR Chennai.

Dr. Nebojsa Bacanin received his first PhD degree in 2014 from the domain of applied computer science, and second PhD degree from Faculty of Mathematics, University of Belgrade in 2015 (study program Computer Science, average grade 10,00). He started University career in Serbia 15 years ago at Graduate School of Computer Science in Belgrade. He currently works as an associate professor and as a Vice-Rector for Scientific Research at Singidunum University, Belgrade, Serbia. He teaches 16 courses on bachelor, master and Ph.D. studies from the domain of computer science.

He is involved in scientific research in the field of computer science and his specialty includes stochastic optimization algorithms, swarm intelligence, soft-computing and optimization and modeling, as well as artificial intelligence algorithms, swarm intelligence, machine learning, image processing and cloud and distributed computing. He has published more than 100 scientific papers in high quality journals and international conferences indexed in Clarivate Analytics JCR, Scopus, WoS, IEEExplore, and other scientific databases, as well as in Springer Lecture Notes in Computer Scienceand Procedia Computer Science book chapters. He has also published 2 books in domains of Cloud Computing and Advanced Java Spring Programming.

He is a member of numerous editorial boards, scientific and advisory committees of international conferences and journals. He is a regular reviewer for international journals with high Clarivate Analytics and WoS impact factor such as Journal of Ambient Intelligence Humanized Computing, Soft Computing, Applied Soft Computing, Information Sciences, Journal of Cloud Computing, IEEE Transactions on Computers, IEEE Review, Swarm and Evolutionary Computation, Knowledge-based Systems, Future Generation Computer Systems, Computer and Information Sciences, SoftwareX, Neurocomputing, Operations Research Perspectives, etc. In 2020 he was designated by prestigious Stanford University list as top 2% researchers in the world.