Comprehensive Trust Based Scheme to Combat Malicious Nodes in MANET Based Cyber Physical Systems

N. Bhalaji and Chithra Selvaraj

Abstract A large scale Wireless Sensor Network (WSN) or Mobile Ad hoc Network is to be definitely integrated into Internet as a backbone of Cyber Physical System (CPS), it is indispensable to believe that Cyber physical systems are free from security challenges, such as the detection of malicious attacks. A trust based model is attributed as an important door to defend a large distributed sensor networks in CPS. Trust is perceived as a critical tool to detect malicious node attacks in distributed computing and communication entities, detection of unreliable entities, and uphold decision-making process of various protocols. In this paper, Trust is invoked between participating nodes to improve the performance of Cyber physical systems by improving the degree of cooperation among them. The proposed schemes are also used to establish reliable path in packet forwarding and route finding. The realism, robustness and effectiveness of the proposed model is validated through a broad set of simulations.

Keywords Trust · Cyber physical system · Security · Malicious attacks · Multicast routing protocol · ODMRP

1 Introduction

Cyber-physical systems merge digital and analog devices, interfaces, networks, computer systems, and they link the natural and unreal physical world. The intrinsic unified and diverse amalgamations of behaviours in these systems make their analysis and design a demanding task [1].

N. Bhalaji (✉) · C. Selvaraj
Department of Information Technology, SSN College of Engineering, Kalavakkam, Tamilnadu 603110, India
e-mail: bhalajin@ssn.edu.in

C. Selvaraj
e-mail: chithras@ssn.edu.in

N. Modi et al. (eds.), *Proceedings of International Conference on Communication and Networks*, Advances in Intelligent Systems and Computing 508,
DOI 10.1007/978-981-10-2750-5_56

Cyber-physical systems (CPS) are concrete and engineered systems whose functions are observed, harmonized, controlled and incorporated around the nucleus of computing and communication. Just as the internet changed how humans communicate with one another, cyber-physical systems will transform how we interact with the physical world around us. Many stately challenges await in the economically vital domains of transportation [2], health-care [3], manufacturing, agriculture [4], energy, defense, aerospace and buildings. The design, construction and verification of cyber-physical systems put forward a massive amount of scientific challenges that must be addressed by an inter-disciplinary community of researchers and academicians. Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability that will surpass the simple embedded systems of today. New smart CPS will drive novelty and contest in sectors such as those mentioned above.

Massive progress has been accomplished in evolving Cyber physical systems during the course of preceding few years. Preliminary technologies are investigated that have spanned an ever-rising set of application fields, endowing breakthrough triumphs in many contrast fields. At the same time, the demand for modernisation in these areas [5] continues to flourish, and is urging the need to step up primary research to keep stride.

Conventional probing outfits are incompetent to manage the full complexity of CPS or amply envisage system performances. For example, trivial outcomes that trip the current electric power grid—an ad hoc system can intensify with startling rate into prevalent power breakdowns. This circumstance epitomises the want for appropriate science and technology to put forward design for the deep interdependencies amid engineered systems and the natural world. The trials and projections for CPS are thus extensive and massive. Novel communication between the cyber and physical constituents demand new architectural models that rewrite form and function. They assimilate the continuous and discrete, compounded by the ambiguity of open environments. Conventional present-day accomplishment assurances are inadequate for CPS when systems are large and spatially, temporally, or hierarchically disseminated in patterns that may quickly alter. With the better autonomy and association possible with CPS, greater possibilities of safety, security, scalability, and reliability are demanded, placing a high premium on open interfaces, modularity, interoperability, and verification [6–8].

Sensors and RFID tags are used as a smart nodes CPS which constitute nerve end of the cyber physical systems and acts as an interface for the data transmission between cyber and physical environments. Smart nodes entrenched with sensors deploy dynamic wireless multihoc environments equipped communication medium like Bluetooth, WiFi, Zigbee protocol etc. in near future huge number of nodes possessing sensing capability and vast number of mobile devices may amalgamate for form a strong CPS. The CPS formed out of the above combination yields

intelligent services to the living community and change the way of their perception towards cyber and physical entities around them. The core communication in CPS is handled by flexible networks like MANET.

The MANET used for the establishment of CPS poses new challenges which are of different from challenges arises in conventional networks. In the later one nodes handles packet forwarding, route selection and data handling whereas networks deployed for the establishment of CPS consists of different class of nodes which are often smart entities. Further architecture constraints, energy utilisation and most importantly low power processing are the highlighting factors which needs more attention in these emerging services which forms the CPS. Wireless nature of MANET make them more vulnerable to non-cooperating behaviour of participating nodes and it is very much possible that nodes may be captured by an adversary which may lead to capture and alteration of data packets. Malicious nodes which became part of the network may damage them by causing falsified routing belief and network partitioning.

2 Generic Trust Functions

Collecting Information: This process involves accumulation of information about nodes participating in the networking functionalities. Primarily the behaviour of the node is monitored to analyse the trustworthiness of it. The decision is arrived based on the information collected either through direct or indirect experience i.e. first-hand experience or through recommendations from it peer members.

Ranking and Routing: Once the above information are collected from the nodes they are categorised into trustworthy nodes and non trustworthy ones. This is achieved based on the trust value obtained with each and every node derived from their present and past functioning. Trust values obtained also acts as an indicator for route selection. Reliable route is chosen where there is less number of malicious nodes prevails.

Node Selection: The nodes with greater trust values are preferred for data transfer. When there is a choice for a node to select its successor among pool of nearby nodes it performs the selection depending upon their trust values.

Transaction: The nodes with higher trust values are chosen for packet transfer and as well given priority in route selection.

Observation: In the above process the node weighs the transaction based on their own experience and collects information about transactions from its nearby nodes too.

3 Trust in Dynamic Networks

Trust is used to identify malicious nodes and employed to guide decision making activity of many protocols in a MANET which is inevitable for performing particular ser of tasks which ends up in increasing collaborations among nodes present. it becomes is necessary to introduce trust among nodes to eliminate malfunctioning nodes from routing path and data transmissions. One way of enhancing security in CPS is to utilise trust to evaluate the trust worthiness of each node participating in the network functionalities. Such trust incorporation into networks not only eradicates the participation of malicious nodes but also increases the overall performance of the networks [9]. The delicate part of computation and judgment of trust is a very challenging task in general and dynamic nature of MANET adds bit more complexity into it. The trust calculations may be initiated between any nodes in the MANET scenario based on direct experience, indirect experience (recommendation) and combination of both [10].

Trust is a security mechanism in conditions where many entities communicate and interact. This trust based security mechanism is derived from the human relationship. Here trust between any nodes cannot be evaluated as it is done in normal societal scenario and needs special attention as stated above in human based society trust is measured up on their activities over the time. The human tend to believe in other human under uncertain conditions depending up on his direct or indirect experience.

Trust is one of the most complex phenomenon in social, business and in digital world. Lot of issues are encountered while imposing and measuring trust in unpredictable networks such as MANET used for establishing CPS. These includes difficulty in evaluating trust in rapidly changing environments and to categorise nodes based on the calculated trust. Wireless networks possess various challenging feature such as energy constraint, dynamic routing and restricted security. CPS based on MANET is prone open to different types of attacks which are introduced due to malicious nodes such as packet dropping attack, Blackhole attack, grey hole attack, duplication and replica attacks.

3.1 Trust Computation

Trust computation leads to various degrees of trustable and non-trustable nodes. In this article trust computation is quantified between 1 and −1. The negative number (−1) represents the degree of distrust, where as positive number represents the complete trust. The number 0 is assigned for the new entrants or unknown node. In this trust model two types of trust are calculated between trustor and trustee nodes.

Trust is a notion of human behaviour. In this article the definition of “Trustor” node refers to the node that implements the trust evaluation and “Trustee” node

refers to the node that is evaluated. Another term mentioned in this test is "Recommender". Such recommender node is the one who provide honest recommendation on a specific trustee to the trustor when demanded.

Direct Trust Direct trust value is calculated basing on the direct experience that trustor nodes possess over trustee node. This direct experience could result in either positive or negative way. The quantity of experience may be unlimited but the computable trust value falls in the range between −1 and +1. To obtain values in the above range hyperbolic sin function a = sinh (b) is used where 'a' represents trust value and 'b' stands for node's direct observation.

In real time a trustor may have several experiences over a trustee node and each experience may impact the trust calculation in either way. The direct trust is calculated as below.

$$\mathrm{DT} = \sinh \sum_{i=1}^{n} P_i \, E_i A_i C_i \tag{1}$$

where,

$$\mathrm{P_i} = \frac{No.\ of\ Packets\ received\ in\ application\ layer\ of\ Trustee\ node}{No.\ of\ Packets\ send\ by\ application\ layer\ of\ Trustor\ node}$$

$$\mathrm{E_i} = \sum\nolimits_{i=1}^{n} \frac{Consumed_i}{Send_i + Received_i + \tau}$$

Energy plays an important role in the successful deployment of MANET in CPS. Energy consumption model is defined as above which dissipates the real scenario where the nodes are being used for the data communication and path finding. In the above sending and receive i indicated the energy consumed by ith sensor while sending and receiving a packet. Consume i denotes the total energy cost of consumption the trust values of the sensor nodes. τ Denotes energy consumption required for the survival of the node.

$$c_i = \frac{No.\ of\ Control\ packets\ received\ successfully}{No.\ of\ Control\ packets\ forwarded\ successfully}$$

When a trustor node doesn't possess enough direct experience on a trustee node, the truster node enquires a third node for recommendation. Let's assume that third node has some trust value IT (indirect trust) on the trustee node basing on its own observation.

Recommended Trust is calculated as

$$\mathrm{RT} = \frac{1}{n} \sum\nolimits_{i=1}^{n} DT * \mathrm{IT}_i \tag{2}$$

where

RT Recommended Trust
DT Direct Trust
IT Indirect Trust

To ensure convincible recommendations a trustor node may enquire more than one third node for recommendations.

Comprehensive Trust calculation

$$CT = DT + (1 + |DT|) * RT \tag{3}$$

where

$-1 \leq \text{DT} \leq 1$
$-1 \leq \text{RT} \leq 1$

When a trustor node obtains direct and recommended trust in this way, a formulae to combine both the values is required to balance the relationship between direct trust and recommendation trust. Impact of recommendation trust depends upon how much direct experience value does the trust verifier holds. If the trust verifier node has no direct experience over a trust prover then the recommendation trust is solely believed.

4 Simulation Results

In this article, an event driven Network simulator [11] is constructed to simulate trust assisted based routing in multicast MANET based CPS. Each experiment is considered as an average of ten different runs and each run is implemented with randomly selected source and destination. The 502.11 DCF is hired as a MAC protocol, and on-demand multicast routing protocol (ODMRP) [12] is as routing protocol. Hundred nodes are randomly located randomly in 1000 * 1000 m simulation area. Sixty traffic pairs with Poisson packet interval are generated. The routing protocol discovers up to 5 routes between source and destination. Maximal route length is 10 hops. The mobility model is the random waypoint model. The velocity chosen falls between 0 and 10 m/s. The average pause time is 250 s. Recommendation trust is handled not more than three hops. The entire schedule of simulation is 2500 s.

Figure 1 depicts the throughput performance results for the traditional ODMRP protocol and Trust enhanced ODMRP protocol in the presence of 5 malicious nodes. The malicious nodes were designed to drop the data as well control packets and the results indicate that the throughput of the traditional protocol rapidly drops with the increase in time when compared to the proposed nodes. When there are no malicious nodes present in the scenario they almost share same throughput thus standing as evidence that trust calculations have very lesser impact over the

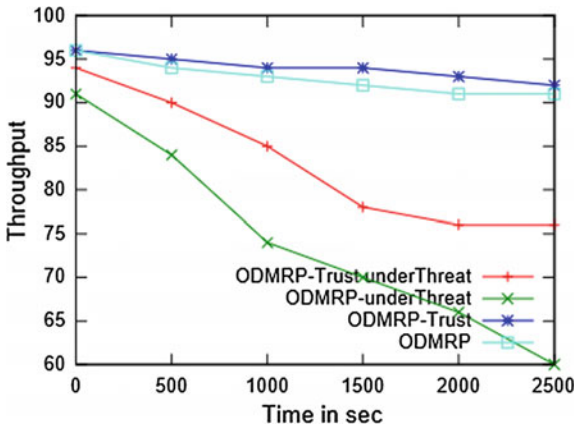

Fig. 1 Network throughput comparison

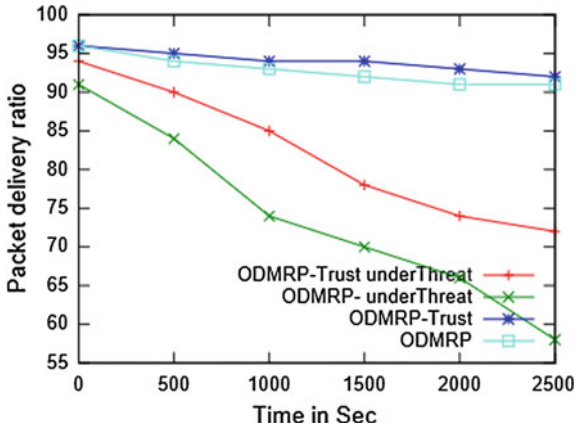

Fig. 2 Network packet delivery ratio

performance of the protocol. In an average 20 % improvement is obtained during the overall simulation duration and it is a very significant improvement considering the dynamic nature of the MANETs.

Figure 2 exhibit the performance analysis of ODMRP protocol's packet delivery ratio with and without trust extensions. The results indicate that the packet delivery ratio of the proposed and existing protocols seems to be same when there are no attackers in the simulation scenario but the situation drastically change as soon as the malicious nodes are brought in. Packet delivery ratio gains an 21 % improvement by employing the trust based route selection when exposed to 5 malicious nodes which drop the packets unintentionally.

5 Conclusion

Trust factors play important role in securing the cyber-physical systems which need to be incorporated from the design phase itself. CPS is opening up exceptional challenges for research and development in several domains. Since MANETs need to be integrated in cyber world to initiate data communication, this article illustrates the necessity of trust assessment in MANET based cyber physical systems. In particular the merits of trust embedded cyber physical systems functioning are simulated through hiring a on demand based multicast routing protocol and the results yielded are immensely encouraging towards further exploration. In future trust based systems will be further compared with the other security providing mechanisms and dedicated protocols may also be deployed for better understanding and evaluation.

References

1. Sanislav, Teodora, and Liviu Miclea. "Cyber-Physical Systems-Concept, Challenges and Research Areas." Journal of Control Engineering and Applied Informatics 14.2 (2012): 28–33.
2. BretHull, Vladimir Bychkovsky, Yang zhang, Kevin Chen, Michel Goraczko, "CarTel: A Distributed Mobile Sensor Computing Systems," in the 4th ACM Conference on Embedded Networked Sensor Systems, Boulder, 2006, pp. 125–138.
3. Insup Lee, Sokolsky. O, "Health Cyber Physical Systems," in 47th ACM/IEEE Design Automation Conference, Anaheim, 2010, pp. 13–18.
4. Meng Zhijun, Zhao Chunjiang, Wang Xiu, Chen Liping, Xue Xuzhang, "Field multi-source information collection system based on GPS for precision agriculture", Transaction of the CSAE, vol. 19, no. 4, pp. 13–18, Jul. 2003.
5. Chaudhary, D. D., S. P. Nayse, and L. M. Waghmare. "Application of wireless sensor networks for greenhouse parameter control in precision agriculture." International Journal of Wireless & Mobile Networks (IJWMN) Vol 3.1 (2011): 140–149.
6. Quanyan Zhu, Craig Rieger and Tamer Basar, "A Hierarchical Security Architecture for Cyber-Physical Systems", IEEE 4th International Symposium on Resilient Control Systems (ISRCS), 2011.
7. Nayot Poolsappasit, Rinku Dewri and Indrajit Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs", IEEE Transactions on Dependable and Secure Computing, 2012.
8. Teodor Sommestad, Mathias Ekstedt and Pontus Johnson, "Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Models", Proceedings of the 42nd Hawaii International Conference on System Sciences, (HICSS), 2009.
9. C Selvaraj., Anand, S.: "Peer profile based trust model for p2p systems using genetic algorithm", Peer-to-Peer Networking and Applications, Vol 5(1), (2012), pp. 92–103.
10. N. Bhalaji, Dr. A. Shanmugam "Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET" Journal of Advances in Information Technology, Vol 2, No 2 (2011), 92–98, May 2011.
11. NS-3. [Online]. Available: http://www.nsnam.org/index.html.
12. S. Deering, D.L. Estrin, D. Farinacci, V. Jacobson, C.-G. Liu, and L. Wei,. The PIM Architecture for Wide-Area Multicast Routing. IEEE/ACM Transactions on Networking, vol. 4, no. 2, Apr. 1996, pp. 153–162.