ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Online - 2455-3891
Print - 0974-2441

Special Issue (April)

Full Proceeding Paper

A GENERIC TRUST MANAGEMENT FRAMEWORK FOR HETEROGENEOUS SENSORS IN CYBER-PHYSICAL SYSTEMS

KANCHANA DEVI V*, GANESAN R

School of Computing Science and Engineering, VIT University, Chennai, Tamil Nadu, India. Email: kanchanadevi@vit.ac.in

Received: 23 January 2017, Revised and Accepted: 03 March 2017

ABSTRACT

Objective: “Wireless technology” is the magic word in today’s era. In which, cyber-physical systems (CPS) is the booming world which binds the physical world and cyber world together. The CPS is also called as safety critical system because of the human life involvement. In this emerging technology, lots of heterogeneous sensors are involved, and each sensor will play an important role. If something goes wrong with sensor or sensor data, it will definitely affect the human life involved in it.

Methods: In this paper, we proposed a generic trust management framework (TRMF) for heterogeneous sensors which will detect the sensor data falsification (data integrity), faulty sensor reading, and packet dropping nodes (selfish nodes) through rules and rating concept.

Results: The efficiency of the proposed framework is evaluated with the help of network simulator 2. The maximum numbers of untrusted nodes are identified in point 0.40 than multi-level trust framework for wireless sensor network and framework for packet-droppers mitigation. It is also evident that TRMF for CPS identifies maximum number of untrusted nodes in the detection range of 0.35 and 0.45. Therefore, 0.35 and 0.45 are considered as maximum and minimum threshold points for effective untrusted nodes.

Conclusion: The experimentation results and comparative study shows that our TRMF will easily detected sensors which misbehave.

Keywords: Cyber-physical systems, Network security, Selfish nodes, Trust management, Wireless sensor network.

DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19631

INTRODUCTION

As we all know that computers or devices are connected using a network mainly to exchange or share the data. There are mainly two broad categories of network one is a wired network and another one is a wireless network. Wireless network is the one which is growing in a drastic manner. In general, the wireless network is very much prone to attacks. In which wireless sensor network (WSN) also prone to many kinds of attacks such as timing attack, the packet dropping attack, cryptographic attack, and data falsification attack.

Fig. 1 shows the overall structure of CPS. Suppose such kind of above attacks hits the cyber-physical system (CPS) where several WSNs are involved to perform the task. Then, it will affect the life of human being who involved in it. It is not at all easy to verify each sensor data individually in such complex environment. Many cryptographic solutions which deal with encryption and decryption are available. However, due to computation overhead, such solution will not suit in this case. That too, if the key sizes are more, then the computation time will also be more. In CPS, the sensors involved will be heterogeneous in nature. It will be very difficult to develop a single cryptographic system for different sensors.

In such environment developing, a trust management framework (TRMF) will be a feasible solution. Trust management in information technology will be used for making decisions. The output of trust management will be 1 or 0. If the value is 1 then the corresponding entity can be trusted or else it will not be trusted. Such decisions can help preventing human life loss due to faulty devices or attackers. In general, trust will differ from application to application. In a heterogeneous sensor environment, developing a trust management for several sensors is not a preferable one. To develop a single framework for all kinds of sensors, few common properties of sensors are examined. Some of the common properties are as follows:

- Turnaround time
- Packet dropping behavior
- Data integrity check
- Cryptographic property.

By checking these properties, we can easily detect whether an attack happened or not, in which each parameter will be assigned a priority. The highest priority goes to data integrity and lowest priority goes to turn around time. Suppose if the data integrity check fails no need to proceed further because it has the highest priority, immediately the trust value will become 0. At the same time, if the turnaround time went wrong or if there is any variation by checking further such as packet dropping behavior, data integrity check, and cryptographic property, we can determine whether it has been attacked by the attacker because of the lowest priority like in Fig. 2

SYSTEM MODEL

In this section, various parameters for trust management such as turnaround time, packet dropping behavior (selfish node), data integrity check, and cryptographic check have been analyzed and given a brief introduction on each property.

Turnaround time

The turnaround time is the total amount of time a packet takes to reach the destination. If the turnaround time is above the allotted threshold value, then it will be considered as the attacker has modified the data or captured the packet.

Packet dropping behavior

Packet dropping is one of the important properties of a WSN to find the malicious node or the compromised node in the network. It is sometimes called as selfish node, which will only receive packets and drop the packets if it is not meant for it mainly to save its energy, where

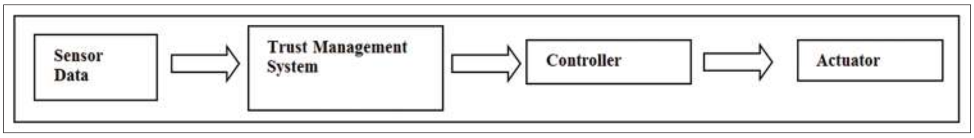

Fig. 1: Overall Structure of cyber-physical system

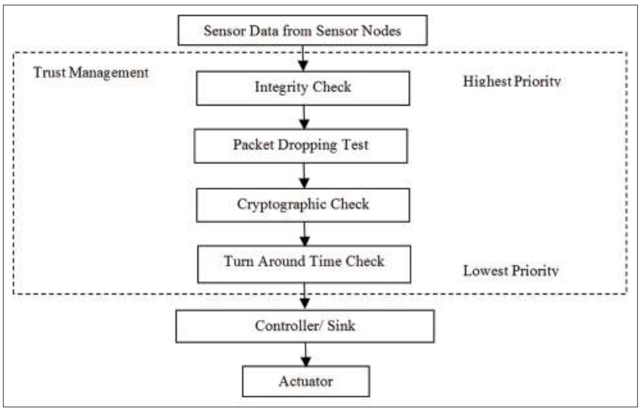

Fig. 2: Trust management framework for cyber physical systems

with the help of sequence number the number of dropped, packets can be determined.

In which a counter variable will be initiated, whenever there is a drop in packets (i.e.) missing sequence number the counter will be incremented. Suppose if the counter, variable goes beyond the threshold value. Then, such node will be considered as untrustworthy node. The threshold value depends on the average number of packets transmitted. Below formula gives the percentage of packet dropped at a node.

$$\text{\% of dropped packets} = \frac{\text{No. of packets transmitted}}{\text{Total No. of packets received}} \times 100 \qquad (1)$$

Data integrity check

Integrity check has been considered as an important property because the data are collected from an open environment and sometimes there will be a need to travel for a longer distance. In such case, there is a chance for the attacker to capture the packet and modifying. This integrity check property will verify whether the data have been falsified or not with the help of watermarking technique. Sometimes this kind of falsifying the data is called as deception attack. In watermarking, there are three steps: First watermarking generation, second embedding the generated watermark along with the data, and third watermarking verification. In watermarking generation, a separate code will be generated from the data itself. Usually, it is called the hashed code. This data along with the hashed code will be encrypted later in cryptographic technique to overcome the problem of tampering. Since this watermarking technique has this much computation part, it is not at all preferable for the sensor nodes.

Initially, data will be collected from sensors, which will be fed into the trust management system. The trust management system will not bother about the type of sensor data because the trust management will work only with the common properties of sensors such as the turnaround time, packet dropping behavior, integrity check, and cryptographic property.

Cryptographic check

Asymmetric key algorithms usually suited for real world usage: The secret key does not need to be shared; the risk of getting the key is very smaller. In an asymmetric key algorithm, each user has to keep only one secret key and a collection of public keys. In symmetric keys, every pair of users' needs to have their own shared secret key which will be used for later transactions. The well-known asymmetric algorithms are relatively slow algorithm (RSA), digital signature algorithm (DSA), and ElGamal. In general, asymmetric algorithms are much slower than symmetric algorithms. Therefore, the combination of both symmetric and asymmetric is being used in many applications. Asymmetric keys are commonly used for authentication purpose, and further one or more symmetric keys are generated and exchanged with the help of asymmetric encryption.

In this way, the above algorithms can be used. Some examples of this type are the IDEA/RSA combination of PGP2 or the BLOWFISH/DSA used in GnuPG. In this type, the RSA is commonly used for encryption purpose which has to be checked for each incoming packets. If the check is not successful, then the packet will be considered as modified by the attacker. Since cryptographic check has been kept as a third level priority (i.e.) third level of the check to calculate the trust value.

Adversary model

In this section, we examine the various scenarios of the adversary model. Definitely the time took to check all these properties will be more and will be an overhead. It can be overcome by checking only the abnormal data packets alone.

Case 1: If suppose the attacker has taken the abnormal data packet and changed it as the normal one, it can be easily identified with the help of turnaround time and cryptographic verification corresponding measure like request for resend can be published.

Case 2: If the attacker compromised any sensor node, it can be identified by calculating the dropped packets property.

Case 3: If suppose the attacker captured the packet and modified, with the help of watermarking verification (integrity check) it can be easily identified.

RELATED WORK

From the past decade, several trust management system has been contributed to deal with the security of CPS. However, none of the approaches has developed a TRMF for heterogeneous sensors. An introduction on an agent-based trust management in *ad-hoc* and sensor network has been made mainly to manage the trust and reputation with minimal overhead in terms of time delay and extra messages. However, the authors have not provided any contribution toward heterogeneous sensors [1]. A collaborative reputation framework has been introduced, in which Watchdog mechanism is used as a detection component and also three approaches have been followed like subjective, indirect and functional reputation [2,3]. A reputation mechanism for identifying malicious nodes using opinion metric has been proposed, in which trust and confidence limit has been estimated by statistical values obtained from the reliable delivery of packets [4]. A novel multiple-level TRMF has been proposed in which there are three trust levels used to implement a trustworthy relationship between nodes. The authors used a subjective trust, an objective trust, and the third one is recommended trust method to get trustable impression from strange nodes [5].

A survey on various trust models has been presented, in which the authors analyzed many trust models such as malicious attacker detection, safe and secure routing, safe and secure data aggregation, secure localization, and safe node selection. Furthermore, the author classifies different attacks against the trust models and concluded like whether the trust models which already exist can resist these attacks or not [6,7]. An analysis has been made for four different decentralized and distributed trust management schemes and proposed a robust M-Trust for mobile P2P networks. The results produced by them possess the outstanding performance in terms of speed, reliability, accuracy, and detection rate [8]. The gaps have been identified and proposed research directions in CPS intrusion detection system based on two terms: First, by detection technique and secondly, through audit material. Furthermore, the authors summarize advantages and disadvantages of both dimensions along with future research area [9]. A semantic model for general information flow analysis in CPS has been proposed and provided an approach to perform the analysis, in terms of trace-based and automated analysis by algebra specification. The authors have taken two models namely gas pipeline and a smart electric power grid system to prove those two preserve confidentiality [10].

A review has been made on some research activities in WSN, in terms of networking issues, coverage and deployment problem. The authors demonstrated how the CPS applications make use of the physical information collected by a WSN to provide a connection between real and cyberspace [11]. A study on trust and reputation management system in wireless communication has been made. The authors have viewed the trust models in two different categories a. Individual level trust Model b. System level trust model, in which incentives will be given to the node to work in ways that enhance the overall system performance. While discussing on the reputation, the authors have mentioned that the neighbor's information will always not be true. It should be taken care in future research [12,13]. A fully distributed trust-based routing framework integrated with optimized link state routing has been proposed. This paper based on Eigen Trust mechanism to identify the packet droppers. Each nodes trust will be transformed into suitable weights provided as input to the optimized link state routing [14].

PROPOSED WORK

As we all know that the main work of sensors is to sense the environment and send the collected/gathered data to the nearby relay nodes to deliver it to the sink. And also, if it is a sensor node, it will process the data and send it to the sink. Later, the data will be a handover to the controller to make decisions like whether to activate the actuator or not. But especially in CPS valuable human being life will get involved. If there is any deviation in the sensed data is not considered properly, it will affect the human life. In such case, trust management plays an important role. In CPS, heterogeneous sensors are involved which will be controlled by distributed controllers to activate the actuators. The role of trust management is to check whether the sensor data can be trusted or not. In order to do so, the node has to undergo various types of checks like time taken to send and receive data are within the limit, whether the sensor node is forwarding the data properly or not, also whether it has followed all cryptographic rule or not, whether the data has modified in between or not. All these checks are common to all heterogeneous sensor nodes. Furthermore, various priority levels are given to each of the checks to reduce the time taken for checking. The highest priority goes to the data integrity and lowest goes to turn around time. Each check will have a threshold value, in which if suppose a sensor data is undergoing various checks, a scaling factor of 10 will be there like in Fig. 3. Furthermore, the scaling factor will be divided into 4 as 2.5 each.

Here, the threshold value will fall at the rate of 5 out of 10. If the scaling value falls within value 5, then the sensor cannot be trusted, it will be considered as it has been compromised by an attacker. Else the sensor node can be trusted. Below the framework for trust management system has been given which starts initially from sensing the data and will pass towards integrity check till turnaround time the result of it will be given to the controller. Fig. 4 shows the flow of data from sensor to controller to make decision to be trusted or not.

Algorithm 1: Trust management
Notations:

SN	Sensor node
N	Network
S	Source
D	Destination/sink
TV	Trust value
A	Weighted average
TV_{th}	Trust threshold value
TF	Total factor
T_{est}	Estimated trust

Algorithm (estimation trust metric)

```
1. For each Sensor Node $SN_i$ in Network N,
2. If $SN_i \in$ Route path $(S, SN_1, SN_2 .... SN_n, D)$
```

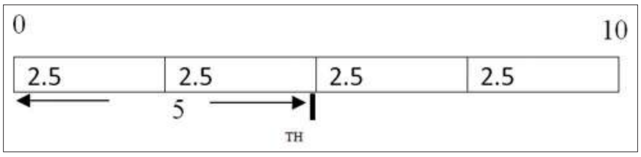

Fig. 3: Scaling factor

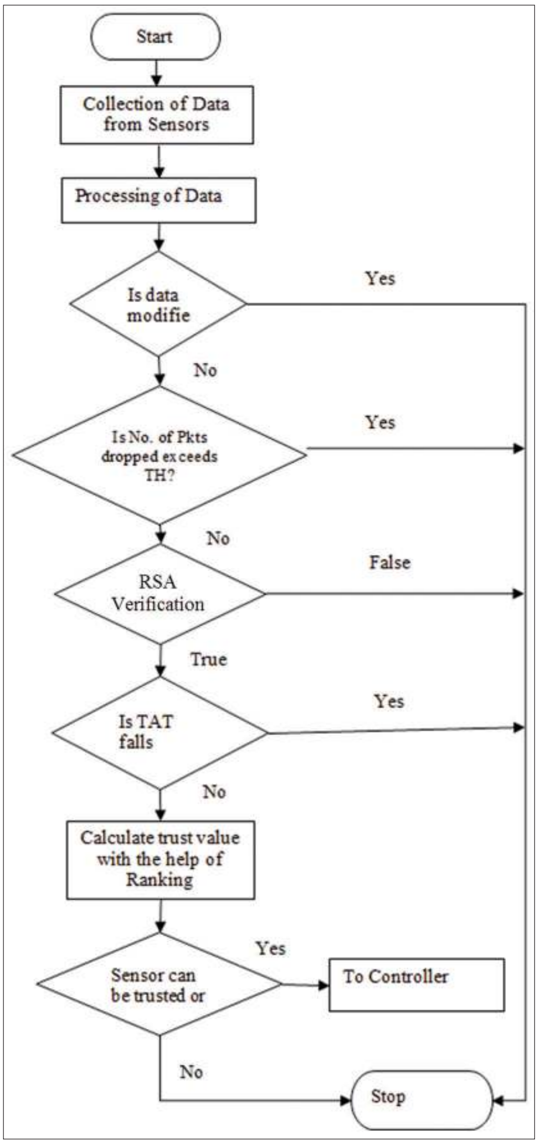

Fig. 4: Workflow diagram

Table 1: Simulation parameters

Parameter	Value
Radio propagation model	Propagation/two-way ground
Network interface type	Phy/Wireless phy
Mac type	Mac/802_11
Interface queue type (IFQ)	Queue/Droptail/Priqueue
Channel	Wireless channel
Link layer type	LL
Initial energy	3.24 Joules
Antenna model	Antenna/Omni antenna
Max packet In IFQ	50
Number of mobile nodes	10
Routing protocol	AODV
X Dimension of topography	600
Y Dimension of topography	600

```
    Set $TV\ (SN_i) \leftarrow 10$ otherwise $TV\ (SN_i) \leftarrow 0$
3.  Compute, the weighted average α as $\frac{TV_{th}}{TF}$
4.  Compute the estimated weight as $T_{est} = \alpha * TV/TF$
5.  If $(T_{est} < T_{th})$
    Assign each Sensor Node $SN_i$ (Untrusted)←True, otherwise $SN_i$(Untrusted)←False
6.  End for
7.  While $SN_i$(Untrusted)←True,
8.  Call omit untrusted node ($SN_i$)
9.  End while
10. End
```

Algorithm 2: Omit untrusted sensor node
Notation:

SN	Sensor node

Algorithm: (Node omission)

```
1. Begin
2. For every route in the network
3. While $SN_i$(untrusted)←True do
4. Omit the sensor node from the path
5. End while
6. Establish new route to the sink
7. End for
8. End
```

Performance evaluation

To simulate the mentioned algorithm to identify the untrusted node, the suitable simulation parameters are identified and tabulated in Table 1. The efficiency of the proposed framework is evaluated with the help of network simulator 2 (NS-2.35). Fig. 5 shows that the maximum numbers of untrusted nodes are identified in point 0.40 than multi-level trust framework for WSN (MTF-WSN) and framework for packet-droppers mitigation (FPDM). It is also evident that TRMF-CPS identifies maximum number of untrusted nodes in the detection range of 0.35 and 0.45. Therefore, 0.35 and 0.45 are considered as maximum and minimum threshold points for effective untrusted nodes.

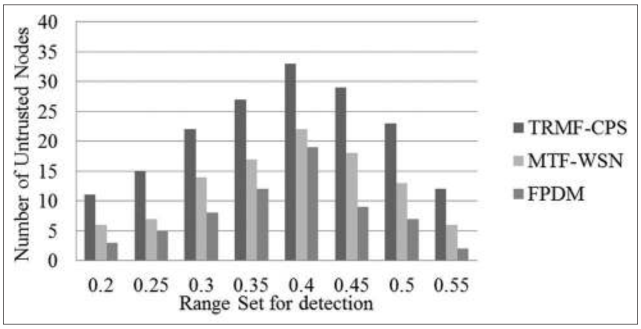

Fig. 5: Comparative chart for trust management framework-cyber physical systems in detecting untrusted nodes

CONCLUSION

In this paper, we have presented a generic TRMF for heterogeneous sensors for finding the untrusted node from the network. Further, the untrusted node will be omitted from the routing path to prevent it from infection spread by the attackers in the network. The proposed framework will identify the untrusted node up to 80% compared to MTF-WSN and FPDM. Extensive, simulations, and analysis have been conducted and demonstrated the efficiency of the proposed scheme.

REFERENCES

1. Ganeriwal S, Balzano LK, Srivastava MB. Reputation-based framework for high integrity sensor networks. ACM Trans Sens Netw (TOSN) 2008;4(3):15.
2. Michiardi P, Molva R. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Advanced Communications and Multimedia Security. US: Springer; 2002. p. 107-21.
3. Zouridaki C, Mark BL, Hejmo M, Thomas RK. A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM. November, 2005. p. 1-10.
4. Boukerch A, Xu L, El-Khatib K. Trust-based security for wireless ad hoc and sensor networks. Comput Commun 2007;30(11):2413-27.
5. Yu H, Shen Z, Miao C, Leung C, Niyato D. A survey of trust and reputation management systems in wireless communications. Proc IEEE 2010;98(10):1755-72.
6. Wu FJ, Kao YF, Tseng YC. From wireless sensor networks towards cyber physical systems. Pervasive Mob Comput 2011;7(4):397-413.
7. Mitchell R, Chen IR. A survey of intrusion detection techniques for cyber-physical systems. ACM Comput Surv (CSUR) 2014;46(4):55.
8. Han G, Jiang J, Shu L, Niu J, Chao HC. Management and applications of trust in wireless sensor networks: A survey. J Comput Syst Sci 2014;80(3):602-17.
9. Zhang B, Huang Z, Xiang Y. A novel multiple-level trust management framework for wireless sensor networks. Comput Netw 2014;72:45-61.
10. Qureshi B, Min G, Kouvatsos D. A distributed reputation and trust management scheme for mobile peer-to-peer networks. Comput Commun 2012;35(5):608-18.
11. Bao F, Chen IR, Chang M, Cho JH. Hierarchical Trust Management for Wireless Sensor Networks and Its Application to Trust-Based Routing. In: Proceedings of the 2011. ACM Symposium on Applied Computing, ACM. March, 2011p. 1732-8.
12. Proto FS, Detti A, Pisa C, Bianchi G. A Framework for Packet-Droppers Mitigation in OLSR Wireless Community Networks. In: 2011 IEEE International Conference on Communications (ICC), IEEE. June, 2011. p. 1-6.
13. Akella R, Tang H, McMillin BM. Analysis of information flow security in cyber-physical systems. Int J Crit Infrastructure Prot 2010;3(3):157-73.
14. Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song YJ. Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans Parallel Distrib Syst 2009;20(11):1698-712.