Inculcating Dynamic Trust Management across Internet through avant-garde Approach

Samia Khan[1] Sherin Zafar[2] Nida Iftekhar[3] Siddhartha Sankar Biswas[4] Gautami Tripathi[5]

{samia.khan20@gmail.com[1], zafarsherin@gmail.com[2],
nida.iftekhar@jamiahamdard.ac.in[3], ssbiswas1984@gmail.com[4],
gautami1489@gmail.com[5]}

Jamia Hamdard, New Delhi-110062

Abstract. In todays' digital era of communication and technology, machines as well as product communicate with each other through a network. So, an essential role is played by trust in various communication therefore it is important that mutual trust must exist among devices to initiate communication or to perform any computational activity in the network. This research paper reviews various trust definitions and present an avant-garde model for trust management that caters the various needs of internet world. This research paper also reviews different trust establishment models and proposes a trust establishment model based on sociological aspects of users in social networks. The proposed model deals with behaviour of users in social network. Model gives deterministic result whether to establish trust with the device so that communication can be initiated among the devices. So the model of trust discussed in this approach provides formal treatment of resilience and accuracy properties of trust through simulation analysis. The dynamic trust-based model adaptively adjust trust as a response to dynamic network changing environment and maximizes the performance of devices.

Keywords: Network, Network attacks, Trust, Trust attacks, Trust Management, Social Networks.

1 Introduction

In today's scenario, communication is happening ubiquitously across all devices although the evolution of internet gave communication a new meaning earlier, communication means interaction however the rise of internet and ICT gave communication a broader meaning encompassing "interaction and computation". This new significance was presented through the development of Ad-hoc arrange particularly mobile Ad-hoc network (MANET), Wireless sensor network (WSN) and Ubiquitous devices). The growth of ICT played an important role in Advancement of communication among heterogeneous devices. Numerous research has been done in the area of communication involving heterogeneous devices in networks such as MANET, WSN etc.

WSNs aggregate an extensive assortment of minor gadgets arranged with fused distinguishing and remote correspondence capacities. Sensor systems used to share some critical qualities with ad hoc systems, for instance they share the requirement for association. [1].

ICIDSSD 2020, February 27-28, New Delhi, India

DOI 10.4108/eai.27-2-2020.2303143

Sensor nodes are used to recognize the event and send the information to the bunch head. Sensor nodes have the restricted assets, constrained calculation and correspondence abilities conveyed in the nature.
The need of securing the communication among these devices is governed by security objectives namely Confidentiality, Integrity, Availability, Authentication, Non repudiation as stated in [3].
To fulfil these security objectives lots of security mechanism were proposed and implemented to ensure that the communication does not get maligned by any attack. All these networks enable communication to take place smoothly on the cost of potential threats, however these threats are enlarging as the technology is growing.
One of the vital essential in beginning correspondence among these system is Trust Management between the imparting gadgets. Trust Management assumes an essential job in these system in light of the fact that the gadgets are heterogeneous, the conveying system is dynamic and strong and there is absence of reliability among the gadgets themselves.
According to the writing the trust is the component of self-reliance in an article. Trust in frameworks is the element of conviction or assurance about interchange center points which are reliant on the historic correspondence. Trust in WSNs might be characterized as, "A consolidated trademark show in WSN for giving dependability, security, protection.
Trust Management is a basic development before gadgets starts correspondence among each other or to play out any computational activity in the framework. Interconnected things, for instance, sensors or mobile phones sense, screen and assemble a wide scope of data regarding human open action. That kind of data can be moreover gathered, consolidated, took care of, researched and mined with the ultimate objective to isolate supportive information to enable clever. Trust administration turns into a noteworthy test in different systems to guarantee solid information investigation, qualified administrations and improved client's security as delineated in Fig. 1.

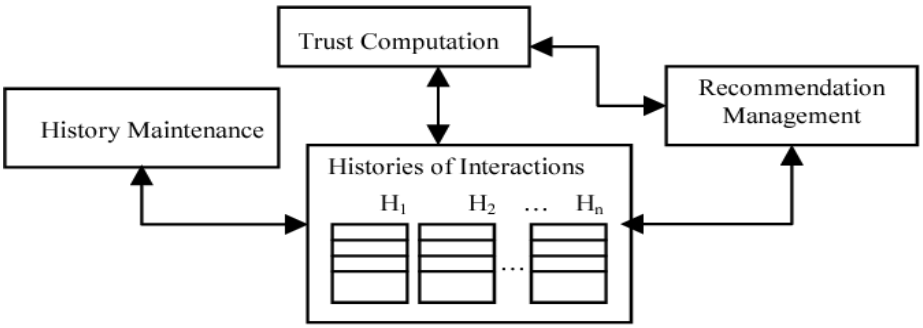

Fig. 1. Trust Administration in Various Networks across Internet [4]

2 Literature Review

Various researches are distributed in the territory of trust the executives demonstrate. In this paper, we completed a small synopsis of 6 research work. The review study of the papers are given below in the Table 1:

Table 1. Literature review of Trust Management in various networks

S.No	Author Name	Paper Title	Year and Published In	Outcome of research
1	Pedro B. Velloso et al.[[5]	Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model	2010 in IEEE Transactions on Network and service Management, Vol. 7	Author proposed a model, which is scalable, which consist of the Trust model architecture and Trust system components. Demonstrate is human-based which assembles a trust connection between hubs in a specially appointed arrange. They have proposed the Recommendation Exchange Protocol (REP) which enables hubs to trade proposals concerning their neighbors. The model can be disengaged in two specific structures Learning plan which is accountable for social event and changing over information into learning and Trust plan that describes the assessment of trust measurement of each neighbor using the learning information given by the Learning structure. In their examination, Scalability of Recommendation Exchange Protocol (REP) is overviewed, considering execution structure and results demonstrate an overhead decay of tolerably 60% with overall no effect at the

				get together rate. They also present the upsides of the proposed relationship advancement in versatile specially appointed systems.
2	Akash Singh et al.[[6]	Security and Trust Management in MANET	2011 in International Conference on Advances in Information Technology and Mobile Communication	Author proposed an algorithm for management of Trust and Security in MANET. The proposed algorithm contains three stages: Initialization, information transmission, and detection. In this algorithm sequential nonce is made at different slot. This methodology is extremely effective to manage different assaults, for example, man in the center assault, detached spying and dynamic obstruction.
3	Hongmei Deng et al. [7]	Building a Trust-Aware Dynamic Routing Solution for Wireless Sensor Network	2010 in IEEE Globecom Workshop on Heterogeneous, Multi-hop Wireless and Mobile Networks	In this paper Author develop Trust aware dynamic routing framework to give a dependable and reliable directing arrangement in unique WSN condition. This model thinks about the self-perception, suggestion notoriety and current data to determine the dependability of neighboring hubs.
4	Hosam A. Rahhal et al. [1]	A Novel Trust-Based Cross-Layer Model for	2011 in National Radio Science Conference	Author Propose a Trust-Based Cross-Layer Model, which use cross-layer thought

		Wireless Sensor Networks		to arrange trust-based model for sensor organizes that guarantee the trust course from source to sink and separate the malignant hub. In the model they utilize the incite and wicked impression of the center points to figure the trust regards and the confirmations from data associate layer and TCP layer for invigorating characteristics. Delineation of this model relies upon two circumstance. In the fundamental they overview the execution of the proposed course of action when the system include colossal number of sensors and found the versatility of the model proposed. While in second situation they assess the model when the measure of vindictive center points increment in the structure, and found that the proposed model work fine paying little mind to whether the percent of threatening is high.
5	Fenye Bao et al. [8]	Dynamic Trust Management for Internet of Things Applications	2012 in International Workshop on Self-aware Internet of Things	Author proposed a Dynamic Trust Management convention for Internet of Things pondering both social trust and QoS trust estimations.

				They took both express perceptions and roaming proposals into record while restoring the trust regards. Their trust the administrators traditions considers a social IoT condition whose circumstance are seriously progressing, e.g., broadening acting insidiously center point people/development, quick investment changes, and cooperation configuration changes.
6	Dong Chen et al. [9]	TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things	2011 at Computer Science and Information Systems, Vol. 8	The proposed trust Management show considers an explicit IoT circumstance containing essentially remote sensors with QoS trust estimations, for example, bundle issuing/transport degree and imperativeness use. Showed up diversely in connection to the past work, it doesn't envision the social affiliations which are through and through major in IoT investments.

3 Research Motivation

3.1 Trust

Trust is the concept utilized in different settings and with various conclusions. Trust on the reliability, capacity, and different characters of an element is a confounded idea in the form of certainty, unwavering quality, trustworthiness, security, and desire [10].Trust has been

considered in various controls going from mind research to software engineering. It is not easy to explain the literal meaning of "trust" in light of the fact that of its compound, associative perspectives. A trust relationship fuses with one another for shared advantage and the setting in which tolerate the trust relationship[11].The establishment or the situation of included substances can be depicted by the information shown. Trust organization is a basic component in frameworks organization systems. A couple of properties of trust when in doubt which depends upon maker's vision and theory are presented underneath.

3.2 Trust Properties

Trust is a confounded thought that have various values relying upon circumstances and the parties involved in the communication and it is dependent on the quantifiable and non-quantifiable elements. Trust is utilized by the people, administration in systems in day by day as an essential element. Trust is influenced by the properties classified into five categories that are shown below in Fig 2.

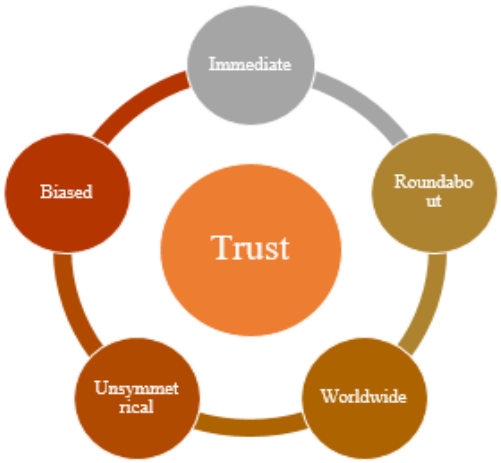

Fig. 2. Trust Properties

3.3 A Significance of Trust Management

Trust Management model are used to ensure secure communication among heterogonous devices. It is very challenging to develop secure communication network among these devices due to resource constraint, dynamic and autonomous characteristics of network. Also several security challenges are present such as attacks on devices, attacks on routing protocols, attacks during data aggregation and storing data etc. Trust management model are used to prevent these kinds of attacks. Several literature have been published which includes Trust management models on these networks [12]. Trust significance include:

- It recognize any vindictive gadget in the system.
- It assist a gadget with calculating trust an incentive for different gadgets in the system. It prevent security threats/attacks and routing attacks.
- It builds dependability of the correspondence.
- It builds the effectiveness of processing assets.

- It builds the heartiness of the system.

3.4 Network Layer attacks in heterogeneous Network

The possible attacks in the network layer in heterogeneous network are given in below TABLE 2:

Table 2. Network Layer attacks in heterogeneous networks

Security Layer	**Attacks in MANET**	**Attacks in WSN**	**Attacks in IoT**
Physical	1. Jamming 2. Eavesdropping 3. Active Interference	1. Jamming 2. Tampering	1. Micro-Probing 2. Device tempering 3. Hijacking Attack
Data Link	1. Selfish Misbehavior of Nodes 2. DOS 3. Misdirecting Traffic 4. Attacking neighbour sensing protocol	1. Collision 2. Exhaustion 3. Unfairness	Layer not present in IoT
Network	1. Worm Hole Attack 2. Black Hole Attack 3. Information Disclosure 4. Byzantine Attack	1. Neglect and Greed 2. Homing 3. Misdirection 4. Black holes	1. Eavesdropping 2. Routing Attacks 3. Traffic Analysis 4. Replication
Transport	1. Session Hijacking 2. SYN Flooding	1. Flooding 2. Desynchronization	1. Node Malfunction 2. Traffic Analysis 3. False Node attack
Application	1. Virus 2. DOS 3. Man in the Middle Attack 4. Impersonation	1. DOS 2. Man in the Middle Attack	1. DOS 2. Cypher text only attack 3. Worms 4. Virus

3.5 Factors affecting Trust

Trust in systems is the level of conviction or certainty about alternate hubs dependent on the specific calculated trust value. There are several factors which affect this trust value:

1. Opinion: It is the convictions or suppositions that are commonly held about one hub to other hub.
2. Past experience: It is the information that is historic.
3. Communion: It is a community of people who share common interest or passion.
4. Straightforward examination: It is the examination of the behaviour of node by another node that attempts to communicate.
5. Proposal: Data provided by the contiguous hub about other hub.
6. Obedience: regardless of whether the trustor and trustee are socially agreeable.
7. Integrity: It is the information that is not altered while communication.

3.6 Security challenges in heterogeneous Networks

Security and protection are the key issues in network and still gigantic difficulties are being confronted with respect to the same. Many new nodes are added to the network and internet which will provide attacker with numerous attack vectors and they can easily perform their evil deed. Human lives and health can become the main target of network attack. Some security challenges are described in Table 3:

Table 3. Security challenges in heterogeneous networks

Challenges in MANET	Challenges in WSN	Challenges in IoT
Scalability	Measuring Confidentiality	Privacy
Insecure Environment	Secure Aggregation	Confidentiality
Lack of Central Authority	Topology Obfuscation	Policy Enforcement
Dynamic topology	Scalable Trust Management	Trust Management
Limited resources	Aggregation with Privacy	Secure Middleware

4 Methodology adopted

In this section we discuss different trust computation metrics used in different trust models [15].

4.1 Trust Calculation Model

Trust calculation procedures are characterized on five plan measurements: Trust configuration, Trust generation, Trust gathering, Trust revise and Trust arrangement.

- Trust Configuration – It incorporates trust traits, for example, nature of administration (QoS) trust and social trust

- Trust Generation – It alludes how to engender trust proof to peers. It contains two trust spread plans, for example, conveyed and brought together.
- Trust Gathering – It alludes to conglomerating trust proof gathered through either self-perceptions or inputs from friends.
- Trust Revise – It concerns when trust is refreshed. It comprise two plans, for example, occasion driven plan and time-driven plan.
- Trust arrangement – Trust arrangement alludes to how to frame the general trust out of various trust properties.

5 Analysis of Trust

This research study focuses on trust management system for which several papers reviewed and highlighted their core work in the literature survey section. Most of research study has treated trust as the most important factor for any kind of vulnerable network for which Trust configuration, Trust generation, Trust gathering, Trust revise and Trust arrangement dimensions are the most specific features. All the research studies focuses in achieving at least three to four components for achieving trust in their system which is depicted in TABLE 4:

Table 4. Research analysis of Trust through its various features

S.No	Author	Trust Configuration	Trust Generation	Trust Gathering	Trust Revise	Trust Arrangement
1	Pedro B. Velloso et al.[5]	✓		✓	✓	✓
2	Akash Singh et al.[6]	✓	✓			✓
3	Hongmei Deng et al.[7]	✓	✓	✓		✓
4	Hosam A. Rahhal et al.[1]	✓	✓	✓		✓
5	Fenye Bao et al.[8]	✓	✓	✓		✓
6	Dong Chen et al.[9]	✓			✓	✓

6 Conclusion

In this survey paper, a broad writing study centers around various networks. This paper starts with an overview about the different networks, for example, WSN, SIOT, MANET etc., and then a literature survey is given on trust management models in various networks. Next, paper address the trust idea and its related concepts including job of trust management in various environment and presented its fundamental properties and significance. And finally, an arrangement is given for various trust calculation models dependent on particular criteria. Authors through this research paper have provided an in depth analysis of trust in any kind of network like WSN, IoT and MANET. The authors in their upcoming work will simulate a trust model and validate through any kind of network through the internet for enhancing trust and belief of users in the network.

References

[1] Rahhal, Hosam A., Ihab A. Ali, and Samir I. Shaheen. "A novel trust-based cross-layer model for wireless sensor networks." Radio Science Conference (NRSC),28th National. IEEE, 2011.

[2] Dhulipala, VR Sarma, and N. Karthik. "Trust management technique in wireless sensor networks: Challenges and issues for reliable communication: A review." CSI Transactions on ICT 5.3, 2017.

[3] William Stallings. “Cryptography and network security principles and practices.” Englewood Cliffs: Prentice Hall PTR, 2006.

[4] Woungang, Isaac et al. “Trust-enhanced message security protocol for mobile ad hoc networks.” IEEE International Conference on Communications (ICC), 2012.

[5] Velloso, Pedro B., et al. "Trust management in mobile ad hoc networks using a scalable maturity-based model." IEEE transactions on network and service management 7.3, 2010.

[6] Singh A., Maheshwari M., Nikhil, Kumar N. “Security and Trust Management in MANET.” In: Das V.V., Thomas G., Lumban Gaol F. (eds) Information Technology and Mobile Communication. AIM, 2011.

[7] Deng, Hongmei, et al. "Building a trust-aware dynamic routing solution for wireless sensor networks." GLOBECOM Workshops (GC Wkshps), IEEE, 2010.

[8] Bao, Fenye, and Ing-Ray Chen. "Dynamic trust management for internet of things applications." Proceedings of the 2012 international workshop on Self-aware internet of things. ACM, 2012.

[9] Chen, Dong, et al. "TRM-IoT: A trust management model based on fuzzy reputation for internet of things." Computer Science and Information Systems 8.4, 2011.

[10] Neeraj, Amitpal Singh. "INTERNET OF THINGS AND TRUST MANAGEMENT IN IOT–REVIEW." International research journal of engineering and technology 3.6, 2016.

[11] Abdelghani W., Zayani C.A., Amous I., Sèdes F. “Trust Management in Social Internet of Things: A Survey. In: Dwivedi Y. et al. (eds) Social Media: The Good, the Bad, and the Ugly.” Lecture Notes in Computer Science, vol9844. Springer, Cham, 2016

[12] Yu, Yanli, et al. "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures." Journal of Network and computer Applications 35.3, 2012.

[13] Li, Wenjia, and Anupam Joshi. "Outlier detection in ad hoc networks using dempster-shafer theory." Tenth International Conference on Mobile Data Management: Systems, Services and Middleware. IEEE, 2009.

[14] Jøsang, Audun & Gray, Elizabeth & Kinateder, Michael. “Analysing Topologies of Transitive Trust.” In: Proceedings of the First International Workshop on Formal Aspects in Security & Trust, 2003.

[15] Guo, Jia, Ray Chen, and Jeffrey JP Tsai. "A survey of trust computation models for service management in internet of things systems." Computer Communications 97, 2017.

[16] Grandsons, T., Sloman, M. “A survey of trust in internet applications.” Communications Surveys & Tutorials, IEEE 3(4), 2000.