A Novel Concept of Trust Node Mapping Using WIMAX NAOH in WLAN

[1]Vivek Kumar Sinha,[2]Kedar Nath Singh

[1]MTech Scholar,[2]Assistant professor
[1]Computer Science Department,
[1]TIT&S, Bhopal, India

Abstract*— *with in the short span of time the WLAN started to emerged,* the novel Concept of the Fifth Generation (5G) wireless communication system started to emerge and it is foreseen that it will be a result of standards convergence. The 5G expectations in terms of scalability and maximum throughput is set much higher when compared with existing technologies e.g. 4G. There are also some challenges and obstacles that has to be addressed by this emerging technologies, like Device to Device (D2D) communication, efficient energy scheme, complete ubiquity and autonomous management .This paper analyses new technologies that could enable 5G networking, discusses potential standardization and development directions, and presents recent research efforts in the area of future mobile networks. *Wi-Max is a broadband remote result that gets to versatile and altered broadband systems through broadband radio access engineering for D2Dcommunication system.

***IndexTerm*— 5G, D2D, HetNet, Trust Node, Neighbor Discovery.**

I.INTRODUCTION

We observe that changes within the field of wireless communications are increasing leaps and bounds. It can be declared that an accelerating evolution of wireless technology together with significantly growing on user demands and expectations. Previous generations of mobile computing and wireless technology establish the foundation for their upcoming future inventions. Existing technologies go far beyond traditional telephony scheme and basic data services that were used by Second Generation (2G) scheme. The 5G of mobile networks is seen as an diagnostic technology ,i.e., one global unified standard that will allow completely seamless connectivity without barriers among both, existing standards and scheme, e.g. Wi-Max and Wireless Fidelity (Wi-Fi),and new wireless systems that are about to emerge. This technology will offer a wide variety of new multimedia services at very high speed. Some emerging services and future applications can be already envisioned, such as augmented reality and tactile Internet. Other examples include the emerging concept of a smart city, steering the traffic of driverless cars or telecommunication support for advanced healthcare management, where patients can be instantly monitored at their houses.

The development in the field of mobile computing and wireless technologies has greatly improved people ability to communicate. These generations of data communication has seen a lot of changes over the time starting from second generation (2G) mobile communication system invented in 1991 to the 3G system first launched in 2001. However, there is continuous incensement in the number of users for subscription for mobile broadband systems.

In the previous generations of cellular networks, D2D communication functionality has not been considered. This is mostly because it has mainly been envisioned as a tool to reduce the cost of local service provision, which used to be fractional in the past based on the cellular operators' market statistics. The operators' attitude toward D2D functionality has been changing recently because of several trends in the wireless market scheme [6]. For example, the number of Context-aware services and applications is growing rapidly. These applications require location discovery and communication with neighboring devices, and the availability of such function will reduce the cost of communication. D2D services can also play a vital role in mobile computing and facilitate effective sharing of resources (spectrum, computational power, applications, social contents, etc.) for users. Service providers can further take advantage of D2D functionality to take some load off of the network traffic locally such as a stadium or a big mall by allowing direct transmission among cellular devices. Device-to-device (D2D) communication allows two nearby cellular devices to communicate with each other in the licensed bandwidth without base station (BS) involved or with partially BS involvement.

Some recent works on D2D in cellular Network have reported results on interference management issues and radio resource allocation [4–6] as well as on communication session setup and Management procedures [3]. In this paper, we provide a categorization of D2D communication and also summarize some major challenges that need to be addressed. Specifically, we briefly discuss security, interference management, and resource allocation schemes, and point out some directions for Future research.

II.DESCRIPTIVE TECHNOLOGIES

5G paradigm requires very high carrier frequencies with massive bandwidths, extreme base station and device densities and unprecedented numbers of antennas. These are the five phases of technology used in fifth generation (5G) to meet the both Architectural and componential challenges [9]:

- Millimeter Wave (mm Wave)
- Massive Multiple Input Multiple Output (MIMO)
- Smarter Devices

- Machine-to-Machine (M2M) communication
- Device-Centric Architecture.

II.1 D2D COMMUNICATION TYPES AND MAIN TECHNICAL CHALLENGES

We project a two-tier 5G cellular network with so-called macro cell and device tiers structure. The macro cell tier structure contains base station (BS)-to-device communications as in a traditional cellular network. The device tier involves D2D communication functionality. If a device connects itself in the cellular network through a BS, this device is must be operating in the macro cell tier structure. If a device connects directly with other device or obtain its transmission through the other devices, these devices must be in the device tier structure.

In macro and device tier structures, the BSs will usually serve the devices continuously. However, at cell edges or congested areas, cellular devices will be allowed to communicate with each other, by creating an ad hoc mesh network structure. In the context of device-tier communications, the operator might have different controlling levels. We can define the following four main types of device-tier communication structure [9]:

II.1.1 Device relaying with operator controlled link establishment (DR-OC):

A device at the edge of a cell or in a weak coverage area can communicate with the BS through relaying its information via other devices. This allows for the device to achieve a higher QoS or more battery life. The operator communicates with the relaying devices for partial or full control link establishment.

II.1.2 Direct D2D communication with operator controlled link establishment (DC-OC):

The source and destination devices exchange data with each other without the help of base stations, but they are assisted by the operator for link establishment.

II.1.3 Device relaying with device controlled link establishment (DR-DC):

The operator is not involved in the process of link establishment. Therefore, source and destination devices are responsible for coordinating communication using relays between each other.

II.1.4 Direct D2D communication with device controlled link establishment (DC-DC):

The end devices will have direct communication with each other without any operator control. Therefore, source and destination devices should use the resource in such a way as to ensure limited interference with other devices in the same tier and the macro cell tier. The design of two-tier cellular system can bring significant improvements over the classical cellular system architecture. This D2D functionality faces many technical challenges, particularly in security and an interference management issues must be resolved. Security must be a major issue that has to be addressed because the user data is routed through other end users' devices. The privacy must be maintained in other devices. One possible solution to ensure security is closed access for the devices that needs to communicate in the device tier structure.

In closed access technique, a device has a set of "trusted" devices, and devices on this list must use the device tier scheme to communicate with each other. For example, the users in a near workplace that acknowledge each other, or the users that have been authenticated via a third party, can directly communicate with each other, managing privacy level. The devices in a group can setup various encryption schemes between each other. In open access, each device acts as a relay for other devices without any restrictions or disturbance. Security issues in D2D functionality involve the process of identifying of potential attacks, threats, and vulnerability points. Some recent works on the security issues of machine-to- machine communication [7–9] can be addressed for open access D2D functionality. For example, the work done by Dong in Kim proposes a trusted environment to establish trust relationships among M2M equipment [7], while secrecy-based access control is discussed in [9].

The Base station can take the edge of the problem of interference management to some extent using centralized methods. On the other hand, in DR-DC and DC-DC, there is no centralized entity to supervise the resource allocation between devices. Operating in the same licensed bandwidth, devices will inevitably impact macro cell users. To ensure the performance of existing macro cell base stations with minimum impact, a two-tier network structure needs to be designed with smart interference management strategies and appropriate resource allocation schemes. Besides the interference between the macro cell and device tiers, there is also interference among users in the device tier.

III. Problem of DC-DC

The major problem of Direct D2D communication with device controlled link establishment are how a device will work as a relay device and also how it will recognize the trusted node with device controlled link establishment. Our main Problem relies on security that comes while communication through relay devices. The main security threat that comes while relaying is:-

I. Confidentiality: The basic security service to maintain the secrecy of important information transmitted between source and destination nodes.

II. Integrity: It should be provided to guarantee that the transmitted messages are not modified by the relays.

IV. Proposed Work

To enhance security features of cellular network system, it is important to evaluate the trustworthiness of participating entity since trust is the major driving force for collaboration. In this paper we present a framework to quantitavely major trust, model trust propagation and defend. In Trust and Reputation (TR) system, network participants try to measure and predict the reliability and trustworthiness of other nodes by evaluating their own experiences and that of others. These systems are usually composed analogous to the flow diagram depicted in Figure 1. A node's own experience from interaction with nodes is combined with knowledge of others and time information via a filter metric the information from others is weighted according to their trust values and the influence of historic information is reduced. After the filter metric calculation a local reputation value is available reflecting the abstract information on how likely a node will behave well with respect to the metric. This value can be very complex representing multiple aspects of trust, such as the trust in fast delivery of a service or the trust to deliver high quality.

Trust definition: Although definitions and classifications of trust have been borrowed from the social science literature, there is no clear consensus on the definition of trust in computer networks. Trust has been interpreted as reputation, trusting opinion, etc [15].

These systems are usually composed analogous to the flow diagram depicted in Figure 1. A node's own experience from interaction with nodes is combined with knowledge of others and flag information. Via a filter metric the information from others is weighted according to their trust values and the influence of historic information is reduced. After the filter of metric the calculation a local reputation value is available.

Figure 1.Trust Node selection & Phase Maintenance

// Nodes directly monitor each other by listening to channel and dynamically update their Trust tables.

1. While timer > initialization period + cluster formation period
2. { Listen to broadcast
3. If node ID is present in trust table
4. Update values for $H^t_{s_{ij}} = (c^t_{s_{ij}}, d^t_{s_{ij}}) \; \forall \; i, j$ where $i \neq j$ and $i, j > 0$ Update Trust metric
5. Update Confidence metric
6. Else discard packet
7. }
8. Periodically execute *Phase Maintenance* Algorithm
9. End;

Abstract information on how likely a node will behave well with respect to the metric. This value can be very complex representing multiple aspects of trust, such as the trust in fast delivery of a service or the trust to deliver high quality.

The maintenance phase involves updating reputation, trust and confidence metrics according to the modeling parameters that we described in this section. In addition, nodes periodically verify the location information of their one hop neighbors. This phase occurs a certain time after the node discovery & trust initialization phase and cluster information period. During this phase the nodes monitor the traffic coming in and out of their neighbors. Periodically, the history of observed outcome is updated by updating. For each of these updates the corresponding trust and confidence metrics are also updated. The trust metric is updated by Computing. The confidence metric is updated by computing equation; periodically the nodes execute the phase maintenance algorithm, as explained in section IV, in order to verify the location information of their one hop neighbors. Figure 2 gives a Description of the Maintenance Phase Algorithm. All networks employing such TR systems are as a consequence subject to new attacks:

• False accusation: Nodes can provide false reports or Accuse nodes of misbehaving. Hereby they can lower the trust rating of highly trusted peers to reduce overall Performance.

• Collusion: Malicious peers report interactions with each other always as highly successful and therefore increase the influence and interaction possibilities of all malicious nodes. Additionally, they can better protect against low trust ratings from correctly behaving peers and are able to harm individual other nodes.

• Identity spoofing: Malicious nodes with a bad reputation value 'capture' the identity of a highly trusted node to obtain its high trust value and therefore receive better service delivery of other nodes with high trust. These attacks are TR system inherent and independent of a specific TR metric or interaction node selection algorithm. They are mainly raised due to a lack of authentication and non-repudiation in standard TR solutions.

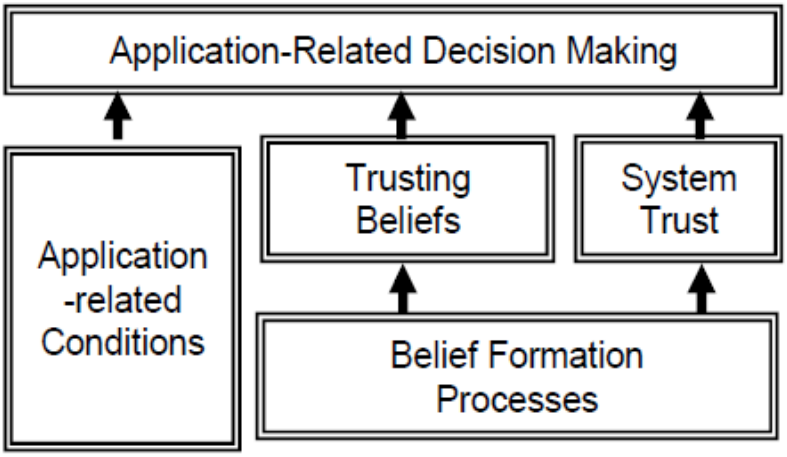

Figure2. Trusts and Reputation Framework

V. Trust Frame Work and Security Analysis

To cope with the aforementioned security issues, we introduce a framework delivering security services such as authentication. The relationship among computing devices is much simpler than that among human beings. The concept of trust in computer networks does not have all six perspectives .Trust behavior, trust intension, situational decision trust and dispositional trust are not applicable to networking. Here, only trusting belief and system trust, which are built upon a belief information process, are relevant to the trust concept in computer networks. In this paper, these three modules are collectively referred to as trust management.

As illustrated in Figure 2, the outcome of trust management is provided to decision making functions, which will make decisions based on trust evaluation as well as other application-related conditions. Further, system trust can be interpreted as a special type of belief, where an entity believes that the network will operate as it is designed. Therefore, the most appropriate interpretation of trust in computer networks is belief. One entity believes that the other entity will act in a certain way, or believes that the network will operate in a certain way. This is our basic understanding of trust in computer networks. The public key is distributed over the network during first interactions of nodes. Furthermore, a node is not limited to generate only one key pair but can also create multiple pairs reflecting multiple IDs. Using these key pairs, a node can leave and re-join the network without losing its ID and is able to (re-)'authenticate' itself to other nodes, when their keying material is distributed. If nodes had successful interactions in the past, they can rely on the nodes identity for further interaction which prevents identity spoofing as one of the main security problems in TR systems [16]. The contributions of the proposed security framework are highlighted through a typical example as depicted in Figure 3: Usually, the user requests a service e.g., a file exchange, data forwarding etc. from the network. The decentralized lookup operation which is application specific, delivers nodes offering that service. This lookup is not always useful or required, e.g. in WMNs the nodes offering data forwarding do not change frequently. The framework is protecting the service requests and offering replies, so that attackers are prevented from offering services in the name of other nodes [5].

Sticking to the example, the metric could be differentiated between trust in delivery, trust in QoS etc. According to the chosen metric a node is selected for interaction and the service is requested in a non-repudiate way (signed). After completion or abortion, the interaction is evaluated and a new trust value is calculated. Finally trust values are updated based on the storage location and validity range of trust values which we call a view.

Direct encounter: Only a node's direct experience is taken as the basis for the trust value used for node selection. As a result, each node has its own, independent trust value for each other node.

• Local View: The nodes include reputation information from the local neighborhood. In this view, neighboring nodes are more likely to have similar, but different, trust values for other nodes.

• Global View: The trust value is calculated and updated at certain centralized spots in the network. For example. In the Trust Me protocol, Secure Bootstrapping Servers (SBS) are used to assign so-called Trust Holding Agents (THA) to joining nodes. Any interaction report is filed to THA peers for compiling an overall trust value [5].

VI. SIMULATIONS AND RESULTS

In this section, we resort to the simulation to evaluate the performance of both the Description of the Node Discovery and Trust Initialization Algorithm and the High Level Description of Maintenance Phase Algorithm one solving the Delay selection through trust management we able to solve the problem of trust management in Device to Device communication in cellular network. The performance gap between these two algorithms is also discussed. The random reusing algorithm is selected as a benchmark in which D2D pairs reuse the resource of uplink cellular user randomly. 10MHz bandwidth communication of WiMax system [14]

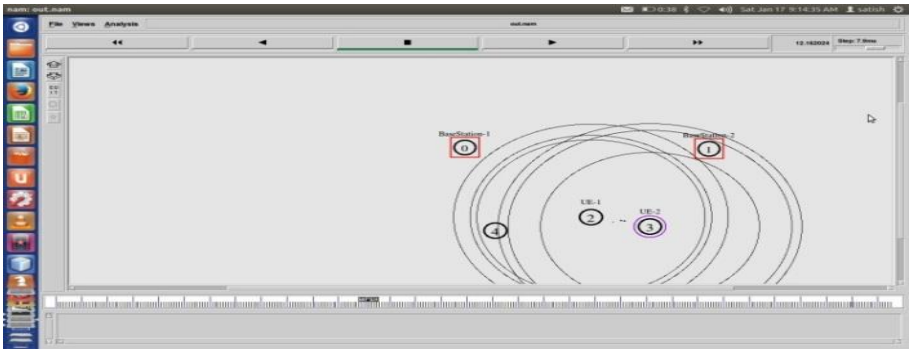

Figure 3. D2D communication

is selected as the simulation condition of D2D communication. Figure 5 table summarizes a list of simulation parameters and their default values.

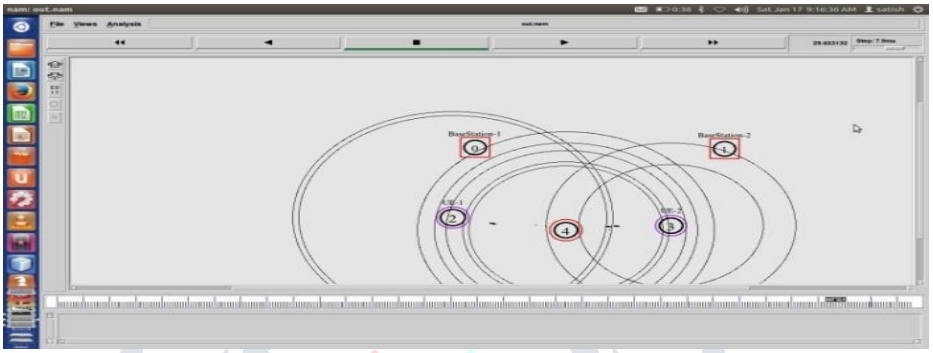

Figure 4. Trust nodes as Relay in D2D

For performance evaluation, we evaluate the channel reusing selection strategy for D2D communications as an underlay to an LTE-Advanced cellular network, where D2D pairs share resources with cellular users. Device to Device Communication performs under simulation parameter of Bandwidth 100Mhz, having maximum Distance of 25m for D2D pair using NS2 WiMax -802.16e patch.

Simulation Parameter

Parameter	Values
Routing Protocol	NOAH
MAC Type	802.16e,WIMAX
Transmission Rang	450M
Topology Size	1300*595
Traffic Type	CBR
CBR Rate	600Kbps
Queue Length	50
Bandwidth	100Mhz
Maximum D2D pair Distance	25m

Figure 5. Simulation Parameter

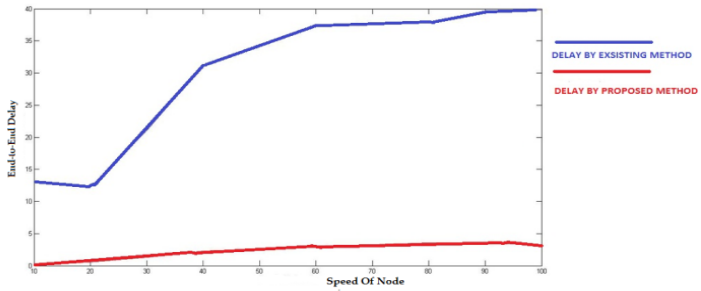

Figure 6. End-to-End Delay

VI. Conclusion and Future Scope

We have proposed a aware trust management based Device to Device communication system that is able to detect and isolate compromised or malicious nodes. Our protocol is design in the context of a relaying node based wireless D2D communication network model with nodes that have unique local IDs. We employ a reputation based Trust Model in Fig (2). We introduce a simple verification protocol that validates reported location information on based of maintains phase algorithm in fig (1). Our protocol is assessed by its ability to detect and isolate compromised nodes. Simulations indicate that our protocol effectively detects and isolate compromised nodes even in the presence of hidden and malicious nodes. In future scope we work on dynamic selection of node as trust relay to make D2D communication more speeder than this.

REFERENCES

[1] Tao Han, Rui Yin, Yanfang Xu and Guanding Yu, Hangzhou 310027, P.R. China2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)-2012.

[2] S. Marti and H. Garcia-Molina. "Taxonomy of trust: Categorizing p2p reputation systems. In Management in Peer-to-Peer Systems", volume 50, pages 472–484, March 2006.

[3] Gu, S. J. Bae, B.-G. Choi, and M. Y. Chung, "Dynamic Power Control Mechanism for Interference Coordination of Device-to-Device Communication in Cellular Networks," in Proc. of IEEE 3rd International Conference on Ubiquitous and Future Networks (ICUFN), Jun. 2011

[4] Daquan Feng, Lu Lu, Yi Yuan-Wu, Geoffrey Ye Li, Gang Feng, and Shaoqian Li"Device-to-Device Communications Underlaying Cellular Networks" in IEEE Transaction on Communication, VOL. 61, NO. 8, AUGUST 2013.

[5] Yiyang Pei, Member, IEEE, and Ying-Chang Liang, Fellow,"Resource Allocation for Device-to-Device Communications Overlaying Two-Way Cellular Networks "in IEEE Transaction on Wireless Communication, VOL. 12, NO. 7, JULY 2013

[6] Xiaohang Chen, Li Chen, Mengxian , Zeng, Xin Zhang, and Dacheng Yang, Wireless Theories and Technologies (WT&T), Downlink Resource Allocation for Device-to-Device Communication Underlaying Cellular Networks in 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC).

[7] Phond Phunchongharn , Ekram Hossain, And Dong InKim,"Resource Allocation of Device to DeviceCommunication underlaying LTE-A Networks" in IEEE Wireless Communications • August 2013.

[8] Osman N. C. Yilmaz, Zexian Li, Kimmo Valkealahti, Mikko A. Uusitalo, Martti Moisio, Petteri Lundén, Carl Wijting "Smart Mobility Management forD2D Communications in 5G Networks" in 978-1-4799-3086-9/14 in 2014 IEEE

[9] Mohsen Nader Tehrani, Murat Uysal, and Halim Yanikomeroglu ."Device-to-Device communication in 5G Cellular Networks: Challenges,Solutions, and Future Directions"IEEE Communications Magazine • May 2014

[10] Youngjae Park and Sungwook Kim"Trust-based Incentive Cooperative Relay Routing Algorithm for Wireless Networks", AICT2014: The Tenth Advanced International Conference on Telecommunications.

[11] Mrs. Chinchu .V. S1 , Ms. Meji Jose2 "Trust Based Secure Payment Scheme for Multi-hop Wireless Networks",e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. VI (Mar-Apr. 2014), PP 38-43.

[12] Tao Han, Rui Yin, Yanfang Xu and Guanding Yu "Uplink Channel Reusing Selection Optimization for Device-to-Device Communication Underlaying Cellular Networks", 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC),pp 42-45

[13] Chih-Lin I, Corbett Rowell, Shuangfeng Han, Zhikun Xu, Gang Li, and Zhengang Pan,China Mobile Research Institute "Toward Green and Soft:A 5G Perspective",IEEE Communications Magazine • February 2014. Pp-12-19.

[14] [Mojtaba Seyedzadegan and Mohamed Othman "IEEE 802.16: WiMAX Overview, WiMAX Architecture", International Journal of Computer Theory and Engineering, Vol. 5, No. 5, October 2013.

[15] D. Gambetta, "Can we trust trust?," in Gambetta, Diego (ed.)Trust: Making and breaking cooperative relations, electronic edition,Department of Sociology, University of Oxford, pp. 213-237, 2000.

[16] Yan Lindsay Sun¤, Zhu Hany, Wei Yuy and K. J. Ray Liu ,"A Trust Evaluation Framework in DistributedNetworks: Vulnerability Analysis and DefenseAgainst Attacks",in Proceedings of MobiCom 2002, Sep 2002.