Security issues in 5G device to device communication

A.S.Khan[1], Yasir Javed[1, 2], J. Abdullah, J.M.Nazim, N.Khan

Network Security Research Group
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak
[2]Prince Sultan University, Riyadh, KSA.

Abstract
5G is a promising technology that will support high connectivity and device to device communication. It also promises to improve the existing technologies and will support them. Existing LTE-A utilize centralized communication scheme where all the authentication mechanisms need to go through the base station. This centralized authentication mechanism may generate authentication and key management overhead as well as computational complexity, thus not in line with the 5G requirements. On the other hand, distributed communication scheme lacks hop by hop authentication, thus, it is challenging to share the initial security credentials within the relay stations at multi-hop.
Secondly, distributed communication scheme required decode and forward relays, a partial intelligent relays that can act as a semi base stations. Such relays are known as non-transparent relays. However, inclusion of such intelligent relays can leads towards a ROGUE RELAY STATION (RRS) attacks, which consequently generate Replay attacks, DoS and the MITM (where mutual authentication is absent). RRS can generate interleaving attack even in the presence of mutual authentication.

Index Terms
Distributed Security Issues; MAC layer issues; Security; Interleaving Attacks; 5G.

1. Introduction

5G appears to be a promising technology in terms of high speed, low latency and ubiquitous connectivity. There are almost 5 billion devices connected and due to IoT storm the number of devices can go up to 25 billion by the year 2020. It will make virtual reality possible by providing instant downloading into 10Gbps and lighting fast response. 5G will provide extremely high throughput with low latency and billions of devices support. It is claimed by Samsung has achieved about 7.5Gbps at static and 1.2Gb/sec in car at 100Km/h while it believes to take car to 50gb/sec, Nokia claims up to 10 Gbps and University of survey claims about 1Tbps. In October 2015 Huawei and Japan NTT managed 3.6 Gbps using 6GHZ band. Huawei claims to make 5G almost 100 times faster than 4G and will support technologies like 4G, LTE, LTE-A, TD-LTE, AVGP, WiMAX TD-LTE-A and LTE with VoLTE and WiMAX [1], [2]. It is pertinent that almost 1.7 trillion Dollars will be invested by operator in 4G by 2020. Network Function Virtualization (NFV), Software defined Networks (SDN) and Heterogeneous Network (HetNets) are already in deployment stages. 4G users consume double or three time the amount of data other than non 4G users due to increase in video stream. Machine-to-Machine communication is also predicted to be 250 million by 2016 while it is predicted to 1 billion and 2 billion by 2020.

5G will provide an opportunity to converge mobile broadband and broadcast services. It is also stated that in 2013 mobile data traffic increased about 81% and expected to increase more than eleven (11) folds by 2018. 5G is challenged to converge both point to point or unicast communication such as mobile TV and point to multi point such as traditional TV. 5G aims to provide a single UAI to meet diverse requirements in terms of application of QoE and Adoption. 5G will allow tactile internet that means that sense of touch along with hearing and seeing capabilities can be achieved like touching and trying clothes before buying, doctor doing operation from America in remote area of Pakistan without any difficulty. Also making possible the augmented reality or virtual reality possible [3].

5G will allow combining both cellular and broadcast industry. In 4G LTE assumes that everything will be packet based or will OFDM, 8011.16m has also similar target as LTE, till 2014 there are 350 commercial vendor of LTE that have reached to 450 by 2015. It will provide seamless connectivity to all devices that are from sensors and actuator to user equipment's. 5G will allow users to connect simultaneously to multiple networks and technologies and there will be multiple concurrent paths for data transfer. 5G will have 3GPP LTE and HSPA and WI-FI as its component [4], [5].

1.1 Definition

5G is being developed by European standard METIS and there is no exact definition of 5G but there are two views given

- 5G is a combination or amalgamation of all previous Generations that are 2G, 3G, 4G and Wi-Fi with higher capabilities in terms of

Manuscript received May 5, 2017
Manuscript revised May 20, 2017

coverage and reliability. It converges these technologies to increase number of devices and calls and promises in providing higher coverage, availability and M2M service.

- ❖ It is a major change to ensure a huge amount of increase in speed and reduction of latency. 5G will be next generation radio access technology with specific target of higher data rate greater than 1Gbps and low latency sub-1ms.

Usually both views are combined as 5G will be combination of both.

1.2 5G technology requirement

There are basic eight requirements of 5G network

- ➢ 1-10 Gbps downlink time practically
- ➢ 1ms end to end delay referred as latency
- ➢ 1000-time increase in bandwidth per unit area
- ➢ 100 times increase in total connected devices
- ➢ Making almost 1000% availability with 0.0001 error chance.
- ➢ Making coverage to be 100%
- ➢ Reducing the energy consumption to 90%
- ➢ Increasing the battery life of machine type devices up to ten years

It is also observed from literature that not even a single use case can cover all requirements. Availability and coverage requirement of 100% is a business decision of operator rather than technical decision. 1000% bandwidth per unit area and 10 – 100% number connections means designing new algorithms to support the small cells and designing mm waves and enhancing the existing network. This requirement will generate load on backhaul in terms of traffic generated and also power requirement will increase. Network energy usage reduction and power reduction will result in green computing and will provided sustainability in terms of economic and ecological industry. Most important requirement is first two that is data rate greater than 10Gbps and latency 1ms in real time. ITU recommends that traffic density will be 10 Tbps/Km2, with connection density of 1 million/Km2, with mobility of 500 Km/h and user experienced data rate will be 0.1 to 1Gbps [4]. The multiplexing will be combination of frequency and time division multiplexing access [4], [5].

2. Key Concepts in 5G Networks

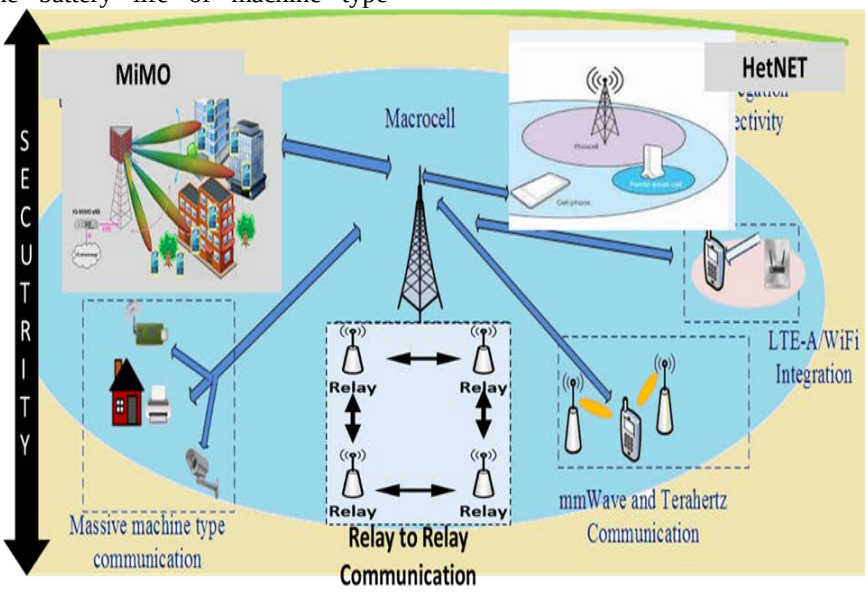

Fig. 1 Showing Key Concepts in 5G Networks

2.1 Spectrum

There will be two ways the spectrum will be used

- ❖ New spectrum and
- ❖ Efficiently using old spectrum.

Current focus is on new spectrum for higher frequency. Proposed model is to use 6GHZ to 300 GHZ bands. Smaller frequency means small radius thus helping to create small cells. For greater distance beam forming is done to end user device and it is able to track mobile users. For cost efficiency spectrum is used wisely.

2.2 Flexible Spectrum management [6], [7]

- ❖ Neutral spectrum bands can be achieved using the

neutral spectrum bands and it can be used in setting up a Radio Access Network (RAT).
- Unused spectrum can be detected by opportunistic spectrum access by secondary users.
- Dynamic sharing of the spectrum in terms of space and time as for ASA/LSA model
- CUS: Spectrum can be used by more than one users simultaneously without need to license

2.3 MIMO

High order MIMO can be used for increasing bandwidth. Multiple transmitters and receivers are used to increase the spectral efficiency of MIMO. Moreover, a single channel is used for transmitting multiple data streams through complex signal processing techniques. It will provide Backward Integration to LTE-A, and will support Wi-Fi to cellular communication as shown in Figure 1 [8], [9].

2.4 LTE

LTE and 4G are not same but now they are being used inter changeably. MIMO and OFDM are important part of LTE. LTE has 14 categories and it data rate starts 1 Mbps for download to 3900 Mbps theoretically only, while upload data rate starts from 1Mbps to 1500 Mbps theoretically only [10], [11]. LTE-Advance is an advance technique that promises a higher data rate about three times than traditional LTE. It has five building blocks (1) channel or carrier aggregation in which 20 different data streams can be combined to one stream (2) MIMO is enhanced from 2x2 to 8x8 antenna system (3) CoMP: Cooperative MIMO allows to receive data from multiple channels to enhance performance. (4) Relay to support communications at edge and (5) HetNets to support multiple small cell in a purpose to increase bandwidth and reduce latency. [11]

2.5 HETNET

HetNet are based on one cellular standard and it may consist of micro, macro, Pico and Femto BSs. [12]. Fusion networks will be used to enhance the performance of heterogonous deployment. Multilayer and multi-stream aggregation is used to have reliable and ubiquitous experience in Fusion Net. In order to lower the risks associated with handoff the host layer manages most of users. SDN is defined by ONF and is used to allocate traffic to network element with intelligence while NFV provide the infrastructure for SDN to run.

2.6 Device to Device & M2M communication

Network of Device to Device like end user equipment's or M2M like Machine sensor and actuator. It will all co-exist with existing infrastructure. Traffic from M2M should be properly assigned without causing congestion thus cognitive intelligence is required.

2.7 Radio Network Planning (RNP)

Radio Network planning is also required to check coverage, capacity and QoS requirements that is to minimize and optimize the location of BSS in selected area using heuristic algorithms for this mmw carrier frequencies are required. In order to go RNP following inputs are required

- Geographical area
- Estimated no of users
- Initial BSS configuration
- Path loss models
- Frequency reuse patterns

When using mmw it opens a large amount of unlicensed frequencies to be used for short range communication. It was already used in WiGIG standard. Spectrum at 28 GHZ can be used to develop small cells as about 80% of subscribers are concentrated in 20% of deployments. Indoor services are largely effected by macro network thus small size cells are required as they can help in getting

- Higher capacity
- Optimized coverage
- Reduced latency
- Reduced round trip delay

2.8 Two Tier Concepts

5G is divided into two-tier architecture in terms of cell location and placement.

First tier called as "Macro cell tier" allows base station to communicate with devices.

Second tier called as "Device tier" will allow device-to-device commutation.

2.9 Cell Size

As mentioned 5G will support variable cell sizes, Macro, Micro, Pico, and Femto

Macro cell will be used to solve initial coverage issues. Pico cell will be used to solve home, enterprise or street capacity and coverage issues. Femto cells will be used home, small enterprise coverage and capacity issues.

2.10 Security

Security is applied vertically that means at each layer security must be ensured. Security is a major concern in 5G, security issues can vary at each layer rising from

simple beacon to complete message, complete discussion is done in Section III [13], [14].

3. Security Issues in 5G

[15] Proposed a reliable, secure and privacy framework for secure vehicle to vehicle communication and created a protocol that is privacy aware and able to report accidents, it will protect the reporting party identity and the data confidentiality through public key encryption over cloud. Result showed that authors were able to receive a secure communication in about one minute.

[16] Focused on confidentiality of data in 5G networks. They argued that physical layer security provides more promising results as it focuses on imperfection of medium and doesn't depend on complexity or computation involved. In 5G, devices will be of adhoc nature that means the devices can join or leave thus security should be provided from end to end. SINR can be used to find problems incurred during transmission. Authors argued of providing closed access to the devices so that only legitimate users are allowed to communicate but new devices may not be capable of handling authorization protocols thus open access techniques can be employed that can be prone to eavesdropping. Author use a techniques of low power communication and movement of receiver to reduce the eavesdropping.

[17] Discussed that how much identity of sender or reporting device is necessary as everything will go through mobile like banking transaction, governmental work or reporting malicious activities. It will require the identity of person to be private and not be able to be tracked. Authors presented an idea of authentication first using EPS-AKA protocols and then sending the key generated using the protocol instead of IMSI number of device. Author used BAN logic to make claims that the result can be promising and require further studies.

[18] Presented a D2D network that has problem of overhearing and eves dropping. Authors used stochastics method to model the network and find SINR ration. Interference between cellular communication and D2D is a major problem for which intelligent scheduling and power control can be user. Cellular communication can be made secure using secrecy coding scheme. Authors used wyner wire-tap channel model in point to point communication for addressing secrecy. They send cooperative jamming signal to avoid the secrecy and showed that physical security can be enhanced with this technique.

[19] Presented an analytical framework for considering security in physical layer in 5G along with Cloud RAN. Authors studied eves dropping on D2D communication with assumption that eve- dropping can be done by devices themselves. The framework will allow users to devices to move far away from commutation area if they feel untrusty connection. Authors designed a technique in which messages will be sent from more channel to avoid overhearing problem. Some messages will be sent from main stream while other will be transmitted on different channel. Authors claimed that this framework will achieve more security in D2D communication.

[20] Presented the 5G technologies in 5G along with device to device communication. In unlicensed like WIFI, Bluetooth can communicate directly device to device but have interference problem. It also raises that in MIMO only TDMA or time division like techniques are considered that is costly as it requires specialized hardware and there are needs to develop low cost multiplexing techniques. Issues of security realized by authors are privacy, integrity, authorization and authentication. This paper only provided challenges around the 5G.

[21] Presented an idea of developing a protocol that can do routing control and key management. The protocol will be having computational cost. In order to establish a secure communication between users the data will be encrypted using a public key cryptography while the key exchange will be done using Deffie-hellman key agreement protocol.

[22] Presented a key exchange security protocols to avoid Man in the middle attack (MITMA) and shared a scenario of distributed denial of service attack. Author presented the idea to protect the device-to-device communication from MITMA where both devices are in a same network area and they are under the coverage of macro station. Authors presented three variations of protocols (1) using Deffie Hellman to exchange public key and then sending the information (2) Using Diffie Hellman to exchange the public key and receive ACK/NACK for the successful delivery of key (3) Using Deffie Hellman to exchange keys while macro station will also send the verification code from data in order to verify the authenticity. Only two node experiments were made and received affordable results.

[23] Raises an issue that Device to Device communication is less secure and requires consideration. IEEE 802.11 the wireless communication protocol is also prone to attacks like Denial of Service attack. Authors presented an idea of legitimacy patterns for continuous authentication. It presented the attacks like jamming or DOS attack that can be done at physical layer while virus and worms attacks are there at application layer. It presented some techniques overview like network coding for D2 security. It also provides an overview of providing security at physical

layer with varying power is better approach. An approach of varying security was developed in which attack yield a score and misdetection of the attack will also be given weight. In this way a continuously evolving approach will be developed to provide security against confidentially and data integrity attacks.

[24] Highlighted the problems of attacks in wireless and no centralized control in D2D communication. In order to provide confidentiality and authentication encryption is required. Authors mentioned that using RSS to generate the key has problem of slowness and can be predicted. Author used channel state information (CSI) that uses 56 pairs of amplitude and phase shift with a variation of using it for nearby subscriber and developed a protocol KEEP that will extract keys using information of all subscribers. It proposed the extraction and combination of keys bits and used hash function to validate the stream. It was able to provide good defense against MITMA.

4. Communication Challenges in 5G

Communication between devices is considered from source to destination, but it may involve no nodes in between (direct communication), Single hop communication or multiple hop communication. Communication that occurs over network can be centralized or distributed, centralized means each message has to go to base station and then to destination while in case of course distributed direct communication or sub-base station communication can occur.

4.1 Relay to Relay Communication

Relay to Relay Communication means that communication can occur between relaying devices, it can be centralized or Decentralized (Distributed) [9] as shown below:

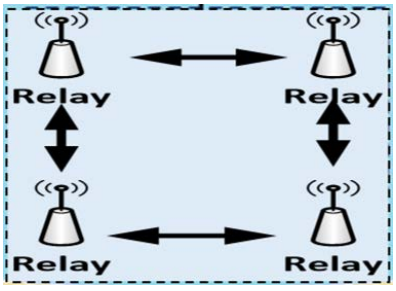

Fig. 2 Showing Relay to Relay Communication

Device to Device (D2D) being a key part to 5G architecture is currently being defined by in LTE REL-12 also called as LTE-B. D2D allows a direct communication between two or more devices without being routed through network after the path authorization is established. It is being controlled by core network. It will allow proximity based applications like using the communication in terms to infrastructure damage. It will also allow have reducing latency and reducing energy consumption. Key benefits of D2D are

- Increase capacity as a spectrum can be shared between users and D2D users.
- It will increase reliability as there will no routing required
- A very high data rate can be achieved due to close proximity that means increased throughput and
- Reduced latency due to communication over direct link and also reducing end to end latency

This technology assumes that users are in proximity to each other and will use the same radio resources. Ericson is a key contributor to D2D research. Vehicle to vehicle communication, service advertisement, offloading of cellular network, intelligent traffic system and public safety are some examples of D2D communication. Following figure shows the basic D2D communication in 5G under the same proximity. D2D communication is done under the network control initially but later it can be fully direct once the trust has been developed. A direct communication will also allow low power consumption and higher data rate. 5G architecture is dividing into two tiers (1) Macro cell tier (2) Device tier [3]

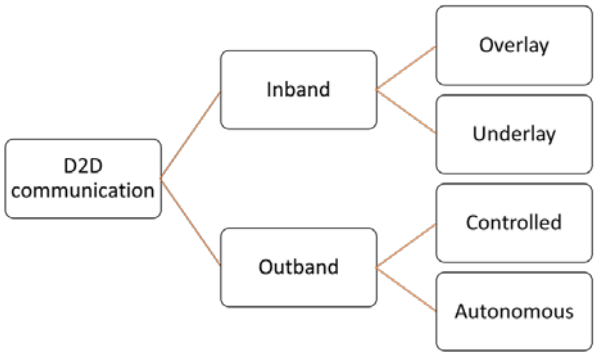

Fig. 3 Showing the types of D2D communication

In Inband communication occurs in licensed spectrum that means both cellular communication and D2D communication occur in licensed spectrum. It has two ways to use (1) Underlay means using the same radio spectrum for cellular and D2D while overlay means using separate channel for cellular and D2D. Inband is more widely used due to increased spectral efficiency and can be used by any device. Its transmission distance is 1km and data rate greater than 1Gbps. Interference management is complex in Inband communication. Outband communication is done using unlicensed band, extra interface is required though some other technologies. In controlled communication, the D2D communication is

controlled by cellular cell while in Inband communication the communication is handled by the D2D devices itself. In Outband transmission rate is lower than Inband but will allow parallel communication on both D2D and cellular network. It will require extra energy and interface and that is overhead on it. [25]

4.2 Challenges of LTE

LTE-A is a mature cellular network in which all the communication goes through Base Station. LTE is also being deployed rapidly and it came as technology first while 5G is still in prototyping phase and lots of research in going on in each direction thus 5G will be a pre-planned technology [29]. LTE doesn't provide pervasive connectivity while 5G is building up on pervasive connectivity for fast access to users. According to literature Centralized mode can support up to 4 relays maximum, with coverage of 3Km practically and Practical coverage of Base Station is 30-60KM as LTE is centralized in nature this heterogeneity will be limited making 5G requirements to be meet that is high data rate and low latency. In order to achieve this 5G are distributed in nature that means that UE that act as relays have partial intelligence and can perform base station tasks. In 5G, the data is decoded, and then forwarded while in distributed nature of 4G LTE the data is amplified form relay and forwarded. [27], [28].

Demand of data is arising currently and it is also making more and more devices connected to network as stated earlier about 5 billion devices are currently connected approximately and is expected to have 25 billion devices connected [30]. The core requirement of 5G is to facilitate hundreds to thousands times better services in terms of data rate, user density, coverage and spectral efficiency. It is also required that user must be confident in terms of the privacy and security at devices and at the communication level. In order to achieve this 5G has to move from centralized to distributed communication. To achieve this distributed communication semi Intelligent Relays are introduced in 5G that will be capable of taking partial decision. Partial decisions will be taken in order to transfer the traffic form source to destination by not forwarding the traffic to base station. Semi intelligent relays are referred as non-transparent relays or decode and forward relays in literature. Practical support for decentralized relays is up to 8 relays. If introduced the semi-intelligent relays, then existing security measure becomes non valid because currently relays are not intelligent but proposed 5G relays will be partially intelligent capable of taking decision. But this kind of communication will also introduce numerous problems in terms of security.

5. Security Issues in Relay to Relay Communication

As stated that 5G will allow intelligent relay communication that will allow distributed communication. These relay will be intelligent but will have couple of security problems. In order to discuss the security issues mainly at MAC layer.

Consider the following scenario as shown in figure 3. There are five (5) relays in the scenario in which every relay can communicate with each other. This scenario doesn't show the devices but it may be assumed that each relay may cater one or more than one device for communication. The figure 3 shows are scenario where Relay no 3 is compromised or have security issues.

It is to be considered that if one of relay becomes there can be various number of threats that can arise as listed below

- Replay Attack: A type of attack in which the valid data is maliciously repeated.
- DOS Attack or Denial of Service attack: A type of attack in which a valid resource is made unavailable.
- Man in the Middle Attack (MITM): Man in the Middle attack where attacker inserts himself maliciously and often alters the communication between two parties.
- Interleaving Attack: A type of attack in which the communication from ongoing communication and will derive authentication from the communication.

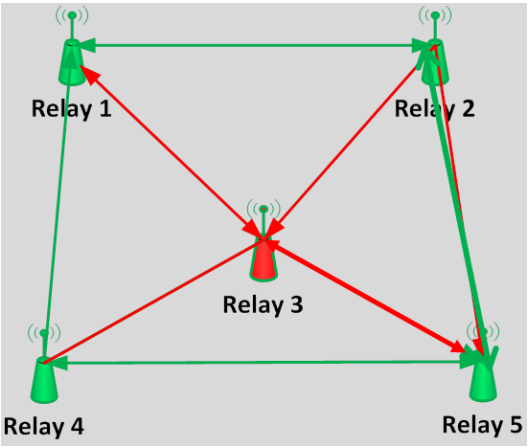

Fig. 3 Security issues in Relay-to-Relay Communication

There are two sorts of communication attacks that can occur in above scenario and as shown in figure 4. In terms of unilateral communication if the one of relay becomes rouge which in this case is relay 3 there will be chances of replay attack that if become successful will result in Man

in the Middle attack or MITM and even if it is not successful will result in Denial of Service or DOS attack.

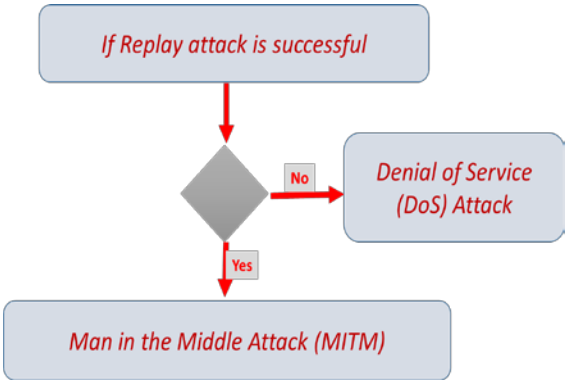

Fig. 4 Replay attack results in DOS or MITM Attack.

The second issue is multilateral authentication that will result in interleaving attack. In Interleaving Attack, Attacker uses two different intelligent sessions between two devices either between

- Base Station and Relay or
- Between Relay and Relay

And availing all the services, if this becomes successful will result in all data loss and may result in wrong data making possible wrong decision. As stated Centralized communication will involve each communication to go through base station.

While Distributed Communication means the communication can be made directly or through intermediate semi intelligent relays.

6. Proposed Solution

This research looks into solution for Distributed Denial of Service (DDoS) or Distributed Denial of Service (DoS) that is special case of DDoS. Some major solution have been discussed and provided in [31] ,[32] that are like Source based mechanism in which action is taken near source of attack that means that each router only allows list of allocated IP's in order to stop the spoofing attack. This is also referred as ingress/egress filtering [33]. Another way is a SAVE Protocol (source address Validity enforcements) that will update routers with allowed list of IP and will block any packet with unexpected IP [34]. Network based Mechanism: Anomaly based detection can be used to detect SYN flood attacks that is occurred when huge amount of SYN messages are flooded making the source drop connection. SYN cookies can be used to avoid this [35]. Destination based Mechanism: When the response is made at destination of attack. (1) Input debugging is used to detect the attack that starts from area of attack to the source using traceroute to find which route is being used as attack [36]. (2) Probabilistic packet marking where router adds their signature to find out the route of illegitimate and legitimate packet. (3) In hash-based IP trace back, hash of each packet is kept at router instead of complete packet using Bloom Filter, it will reduce the memory requirement too [37]. Distributed mechanism: Active internet Traffic Filtering enables the receiver to contact the source and ask him to stop misbehaving [38]. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) can be used at application level to apart computers and humans [31], [39]. Continuous Authenticity and legitimacy patterns where the encoding secret key is not kept same and changed with time in a pattern, it will not allow the traffic to be compromised even if the first key is broken or compromised [40]. Even a Scoring mechanism can be used to allocate the traffic a value that will be done on based of violation [40].

KEEP protocol that works on shared secret key between two parties and use Channel state information for sharing and extraction of key [41]. Diffie-Hellman Key Exchange is used for secure communication for secure communication is proposed to share the communication and will only allow authenticated user for communication [42]. Diffie-Hellman and public key cryptography is used in LTE-A network where communication is handled by Gateway so that communication is secure and nodes are always available as well as for non-availability [43]. Diffie-Hellman key Exchange protocol is being used by public key exchange and all other communication is done in encrypted way adding the Head in communication for approval. It is used to secure DoS and MITM attack in 5G network between two devices [44].

All these solutions discussed mostly are employed in 4G/ LTE network except [44] that take a partial case of 5G communication in which two devices that want to communicate using similar kind of application. Thus there is a need of complete secure solution for DoS attacks that can handle other attacks too and is light in weight.

In order to understand the problems, this study tends to figure out the issues that can occur due to centralized communication and may result in data security issues that did not exist in older communication.

For this a bi-direction authentication mechanism is proposed that will do key management too. This mechanism will support the authentication in distributed relay-to-relay communication as shown in figure3.

The proposed authentication and key management guidelines should be compatible with intelligent relays based communication in R2R 5G cellular networks.

The proposed guideline should also be lightweight to reduce authentication overhead by using distributed hop-by-hop authentication and localized key management to ensure 5G requirement of low latency and high throughput is met. The designed protocol will be able to handle Denial of service, Man-in-the-middle, replay and interleaving attack.

So this study propose an algorithm as shown below where if device need to communicate then each device has to ask the relay R to prove its identity from Base station (BS) that uses Diffie-Hellman key exchange to inform the validity of Relay(R) to Device (D). Moreover, each communication is made through secret key encryption so that traffic is kept secret and cannot be read. There are chances that the key can be compromised so in order to avoid this Change function is also shared in initial message that will tell the devices to change the key value after defined time so that even if the key is compromised there is no problem. Change function and Time span is set by Sender.

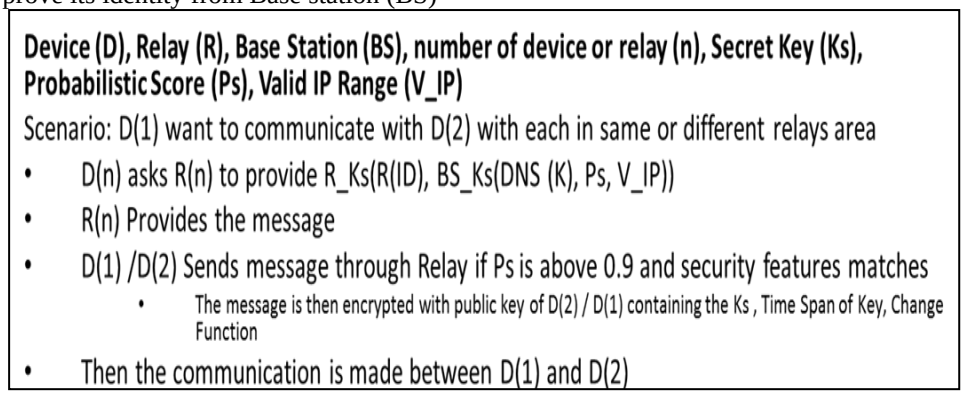

Fig. 5 Secure Communication Proposed Algorithm

The Relay (R) trust is managed by probabilistic model in which reporting mechanism exists that will allow devices D or Relays R to report about Rouge Relay for this algorithm shown in Figure shows a blueprint of protocol. BS runs security routine if it finds a problem then according to problem level the security value is set, if there is none then only reporting device is informed that there is no problem. It is still if an alternative route is available, the route is changed. If there is fault all nearby nodes and relays are informed to block the traffic from Relay (X) that is reported. Moreover, in order to stop IP spoofing only a range of Valid IP (V_IP) is allowed so that to avoid spoofing attacks.

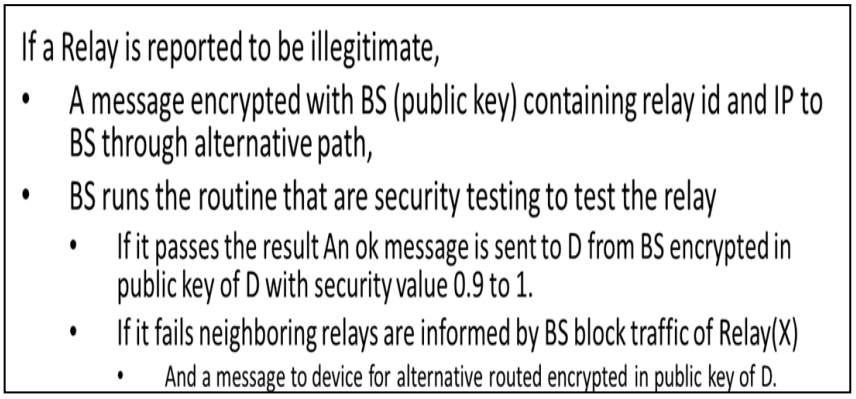

Fig. 6 Reporting A Rouge Station in Proposed Algorithm

It will avoid the DDoS, MITM and interleaving attacks in 5G networks, as in 5G major requirement is that it will provide a secure and light weight connectivity that will incresea the total bandwidth. It is shown that new challenges that were not there in centralized communication has raised but proposed algorithm will be able to handle the problems raised by Distributed communication. In future, the work will presented a proof of study with experimental results.

To the future researches in area of security, this work can provide a core framework for any distributed security

protocol development in 5G.

Acknowledgement

This work is funded by the Research and innovation Management Center, Universiti Malaysia Sarawak under the grant no. F08 (S150)/113/21014(15).

To the future researches in area of security, this work can provide a core framework for any distributed security protocol development in 5G.

References

[1]. Khan, A. S. (2014). "Secure and efficient distributed relay-based rekeying algorithm for group communication in mobile multihop relay network." International Journal of Communication Networks and Information Security **6**(3): 189-199.

[2]. Khan, A. S., N. Fisal, Z. A. Bakar, N. Salawu, W. Maqbool, R. Ullah and H. Safdar (2014). "Secure authentication and key management protocols for mobile multihop WiMAX networks." Indian Journal of Science and Technology **7**(3): 282-295.

[3]. Khan, A. S., N. Fisal, N. N. M. I. Ma'arof, F. E. I. Khalifa and M. Abbas (2011). "Security issues and modified version of PKM protocol in non-transparent multihop relay in IEEE 802.16j networks." International Review on Computers and Software **6**(1): 104-109.

[4]. Khan, A. S., N. Fisal, S. K. S. Yusof, S. H. S. Ariffin, M. Esa, N. N. Maarof and M. Abbas (2010). An improved authentication key management scheme for Multihop relay in IEEE 802.16m networks. 2010 In the Proceedings of IEEE Asia-Pacific Conference on Applied Electromagnetics, (APACE 2010), Port Dickson, Malaysia, 2010.

[5]. Khan, A. S., H. Lenando and J. Abdullah (2014). "Lightweight message authentication protocol for mobile multihop relay networks." International Review on Computers and Software **9**(10): 1720-1730.

[6]. Khan, A. S., H. Lenando, J. Abdullah and N. Fisal (2015). "Secure authentication and key management protocols for mobile multihop WiMAX networks." Jurnal Teknologi **73**(1): 75-81.

[7]. Khan, A.S., Abdullah, J., Lenando, H., Nazim, J.M. Green resource allocation for multiple ofdma based networks: A survey (2016) Journal of Electronic Science and Technology, 14 (2), pp. 170-182.

[8]. Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C. (2014). What will 5G be?. IEEE Journal on selected areas in communications, 32(6), 1065-1082.

[9]. Baker, M. (2009). LTE-Advanced physical layer. In Proc. IMT-Advanced Evaluation Workshop, 3GPP, Beijing (pp. 1-48, December).

[10]. Moskvitch, K. (2015). Tactile Internet: 5G and the Cloud on steroids. Engineering & Technology, 10(4), 48-53.

[11]. Gupta, A., & Jha, R. K. (2015). A survey of 5G network: architecture and emerging technologies. IEEE access, 3, 1206-1232.

[12]. ITU1R, M. IMT vision1framework and overall objectives of the future development ofIMT for 2020 and beyond (Vol. 5). S. 1.]: ITU Working Document.

[13]. Demestichas, P., Georgakopoulos, A., Karvounas, D., Tsagkaris, K., Stavroulaki, V., Lu, J., ... & Yao, J. (2013). 5G on the horizon: key challenges for the radio-access network. IEEE Vehicular Technology Magazine, 8(3), 47-53.

[14]. Kela, P., Costa, M., Salmi, J., Leppanen, K., Turkka, J., Hiltunen, T., & Hronec, M. (2015, May). A novel radio frame structure for 5G dense outdoor radio access networks. In 2015 IEEE 81st Vehicular Technology Conference (VTC Spring) (pp. 1-6). IEEE.

[15]. Oshin, O. I., Luka, M. K., & Atayero, A. A. (2016). From 3GPP LTE to 5G: An Evolution. Accepted, Transactions on Engineering Technology--WCE2015, Springer, Jan.

[16]. Lee, J., Kim, Y., Kwak, Y., Zhang, J., Papasakellariou, A., Novlan, T., ... & Li, Y. (2016). LTE-advanced in 3GPP Rel-13/14: an evolution toward 5G. IEEE Communications Magazine, 54(3), 36-42.

[17]. 3GPP (2015). 3GPP TS 36.306 (2015-03)

[18]. Dahlman, E., Parkvall, S., & Skold, J. (2013). 4G: LTE/LTE-advanced for mobile broadband. Academic press.

[19]. Boccardi, F., Heath, R. W., Lozano, A., Marzetta, T. L., & Popovski, P. (2014). Five disruptive technology directions for 5G. IEEE Communications Magazine, 52(2), 74-80.

[20]. Hu, F. (Ed.). (2016). Opportunities in 5G Networks: A Research and Development Perspective. CRC Press.

[21]. Chen, M., Qian, Y., Mao, S., Tang, W., & Yang, X. (2016). Software-defined mobile networks security. Mobile Networks and Applications, 1-15.

[22]. Hashem Eiza, M., Ni, Q., & Shi, Q. (2016). Secure and privacy-aware cloud-assisted video reporting service in 5G enabled vehicular networks. IEEE Transactions on Vehicular Technology.

[23]. Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J., & Di Renzo, M. (2015). Safeguarding 5G wireless communication networks using physical layer security. Communications Magazine, IEEE, 53(4), 20-27.

[24]. Choudhury, H., Roychoudhury, B., & Saikia, D. K. (2012, June). Enhancing user identity privacy in LTE. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on(pp. 949-957). IEEE.

[25]. Ma, C., Liu, J., Tian, X., Yu, H., Cui, Y., & Wang, X. (2015). Interference exploitation in D2D-enabled cellular networks: A secrecy perspective.Communications, IEEE Transactions on, 63(1), 229-242.

[26]. Ghanem, S. A., & Ara, M. (2015, February). Secure communications with D2D cooperation. In Communications, Signal Processing, and their Applications (ICCSPA), 2015 International Conference on (pp. 1-6). IEEE.

[27]. Chin, W. H., Fan, Z., & Haines, R. (2014). Emerging technologies and research challenges for 5G wireless networks. Wireless Communications, IEEE, 21(2), 106-112.

[28]. Jung, Y., Festijo, E., & Peradilla, M. (2014, May). Joint operation of routing control and group key management for 5G ad hoc D2D networks. In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on(pp. 1-8). IEEE.

[29]. Sedidi, R., & Kumar, A. (2016, March). Key exchange protocols for secure Device-to-Device (D2D) communication in 5G. In 2016 Wireless Days (WD)(pp. 1-6). IEEE.

[30]. Abualhaol, I., & Muegge, S. (2016, January). Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 5763-5771). IEEE.

[31]. Xi, W., Li, X. Y., Qian, C., Han, J., Tang, S., Zhao, J., & Zhao, K. (2014, May). Keep: Fast secret key extraction protocol for d2d communication. In Quality of Service (IWQoS), 2014 IEEE 22nd International Symposium of (pp. 350-359). IEEE.

[32]. Wang, M., & Yan, Z. (2016). A Survey on Security in D2D Communications.Mobile Networks and Applications, 1-14.

[33]. Onoe, S. (2016, January). 1.3 Evolution of 5G mobile technology toward 1 2020 and beyond. In 2016 IEEE International Solid-State Circuits Conference (ISSCC) (pp. 23-28). IEEE.

[34]. Golrezaei, N., Dimakis, A. G., & Molisch, A. F. (2012, December). Device-to-device collaboration through distributed storage. In Global Communications Conference (GLOBECOM), 2012 IEEE (pp. 2397-2402). IEEE.

[35]. Zhou, B., Hu, H., Huang, S. Q., & Chen, H. H. (2013). Intracluster device-to-device relay algorithm with optimal resource utilization. IEEE transactions on vehicular technology, 62(5), 2315-2326.

[36]. Ramadan, M., Li, F., Xu, C., Mohamed, A., Abdalla, H., & Abdalla, A. (2016). User-to-User Mutual Authentication and Key Agreement Scheme for LTE Cellular System. International Journal of Network Security, 18(4), 769-781.
[37]. Alliance, N. G. M. N. (2015). 5G white paper. Next generation mobile networks, white paper.
[38]. S. T. Zargar, J. Joshi, D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks", IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046-2069, 2013.
[39]. S. Ranjan, R. Swaminathan, M. Uysal, E. W. Knightly, "DDoS-resilient scheduling to counter application layer attacks under imperfect detection", Prof. IEEE INFOCOM, pp. 1-13, Apr. 2006.
[40]. P. Ferguson, "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing", 2000.
[41]. J. Li et al., "SAVE: Source address validity enforcement protocol", Proc. IEEE INFOCOM, vol. 3, pp. 1557-1566, 2002.
[42]. T. Peng, C. Leckie, K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems", ACM Comput. Surveys, vol. 39, no. 1, pp. 1-42, Apr. 2007.
[43]. R. Stone et al., "Centertrack: An IP overlay network for tracking DoS floods", Proc. USENIX Security Symp., vol. 21, pp. 114-128, 2000.
[44]. C. Snoeren et al., "Hash-based IP traceback", SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3-14, 2001.
[45]. Kolupaev, J. Ogijenko, "Captchas: Humans vs. bots", IEEE Security Privacy, vol. 6, no. 1, pp. 68-70, Jan. 2008.
[46]. K. Argyraki, D. R. Cheriton, "Scalable network-layer defense against Internet bandwidth-flooding attacks", IEEE/ACM Trans. Netw., vol. 17, no. 4, pp. 1284-1297, Apr. 2009.
[47]. Abualhaol, I., & Muegge, S. (2016, January). Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns. In System Sciences (HICSS), 2016 49th Hawaii International Conference on (pp. 5763-5771). IEEE.
[48]. Xi, W., Li, X. Y., Qian, C., Han, J., Tang, S., Zhao, J., & Zhao, K. (2014, May). KEEP: Fast secret key extraction protocol for D2D communication. In Quality of Service (IWQoS), 2014 IEEE 22nd International Symposium of (pp. 350-359). IEEE.
[49]. Shen, W., Hong, W., Cao, X., Yin, B., Shila, D. M., & Cheng, Y. (2014, December). Secure key establishment for device-to-device communications. In Global Communications Conference (GLOBECOM), 2014 IEEE (pp. 336-340). IEEE.
[50]. Zhang, A., Chen, J., Hu, R. Q., & Qian, Y. (2016). SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks. IEEE Transactions on Vehicular Technology, 65(4), 2659-2672.
[51]. Sedidi, R., & Kumar, A. (2016, March). Key exchange protocols for secure Device-to-Device (D2D) communication in 5G. In Wireless Days (WD), 2016 (pp. 1-6). IEEE.