Research on Secure D2D Communication using Lightweight Cryptographic Techniques

Ajith Kumar V, K Satyanarayan Reddy

Abstract:Outgrowth of wireless mobile communication lead to new revolution. Smart phones are making inroads into socio economic realms. Today we use smart phones almost like a personal computer. Some important milestones have been witnessed, such as number of fixed line Telephone connection has been surpassed by number of mobile phone connection, Number of connected/IP enabled devices in home surpassed more than one per person. In nutshell, people are living in a connected world, trying to connect unconnected things. Devices are becoming intelligent, smart and connected. Need for Device to Device communication is growing every day. D2D communication is becoming popular in health care , disaster or emergency services, power grid and lot many. Security cannot be undermined as D2D communication is becoming pivotal and impacting larger part of our life. In this paper our focus is on security challenges in D2D communication and explore remediation with lightweight cryptography. In this paper an effort has been made to study various techniques for securing D2D communication. This paper focuses on securing D2D communication using lightweight cryptographic algorithms.

Keywords:D2D Communication, Federal Information Processing Standard, Lightweight Cryptography, National Institute of Standards and Technology, User Equipment.

I. INTRODUCTION

Device-to-Device(D2D) communication in wireless cellular net-works [1] is considered as the direct communication between two users without using the Base Station (BS) or core network. D2D communication in recent years crated lot of interest in Academia and Industry, surveys have been conducted by researchers exploring various possibilities of using D2D communication, such as disaster recovery, emergency services. Our contribution is, visited existing work on secure D2D communications. Analyzed them with respect to standard security requirements identified by the researchers such as Confidentiality, Integrity and Availability, Authentication, Non-repudiation, Privacy and various security attacks Denial of Service (DoS), Man-in-the-Middle, Replay attack, Identity disclosure, etc. Majority of the current work focuses on authentication, authorization of the end users and devices using traditional cryptographic techniques, however we are looking at providing security for the data in transit. We strongly believe that there is a scope for using lightweight cryptographic techniques to enhance security and increase the performance. This paper is organized as follows. Introduction, Section 2 focuses on classification of D2D communication, Section 3 deals with security requirements of D2D communication, here elaborate discussion is made on security requirements, various attack scenarios been identified. Section 4 covers the various works that has been carried out for ensuring security in D2D communication with a focus on lightweight cryp-tographic techniques. Section 5 conclude with identified research areas.

II. EVOLUTION OF D2D COMMUNICATION

D2D communication in cellular networks [2] is defined as direct communication between two mobile users without traversing the Base Station (BS) or core network. Device to Device communica-tion is wireless and is different compared to Mobile Ad-hock Net-works (MANETS). Fig.1 shows the classification of Device to

Device communication. Basically, D2D communication can be broadly classified into two major categories. Inband D2D commu-nication and Outband D2D communication.Inband D2D commu-nication further classified into Underlay and Overlay. Underlay uses same radio resources for cellular communication and D2D communication, however, in this case there are some issues like interference and resource allocation. Researchers working in this area have proposed various algorithms for resolving interference issues, however in case of Overlay communication, it uses dedicated radio resources. Outband D2D communication does not use the same wireless channel for D2D, instead uses Wi-Fi Direct/Blue tooth/Zig-bee. In this research work, our focus is Outband D2D communication, hence D2D nodes should have 2 radio links one for Wireless and another for D2D communication using Wi-Fi Direct/Bluetooth/Zig-bee etc.

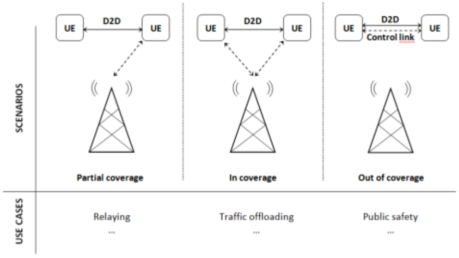

Fig. 1: Uses cases of D2D Communication [18]

Outband D2D communication can be further classified into Con-trolled D2D communication, where Service Provider controlled the second link, in case of Outband Autonomous D2D communication second link which is used

Revised Manuscript Received on June 10, 2019.

Ajith Kumar V, Research Scholar, Department of Computer Applications, Regional Research Centre, VTU Belguam,Karnataka, India (Email: ajith.it@gmail.com)

Dr. K Satyanarayan Reddy Professor Department of ISE,CAMBRIDGE INSTITUTE OF TECHNOLOGY (affiliated to VTU Belgaum),Bangalore, Karnataka, India

for D2D communication is controlled by end user not by the service provider. There are some challenges and advantages in D2D communication. Advantages are off-loading the communication from the centralized entity, saving the spectrum and bandwidth. Short range communications are typically characterized by higher throughput, lower delay and energy consumption when compared to long range communications [2].

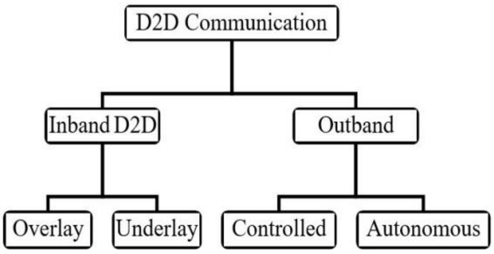

Fig. 2: Device to Device Communication Classification [1]

2.1. Classification of D2D Communication

D2D communication can find applications in three scenarios.

- **In Coverage or Full Coverage:** This is the scenario, where User Equipment (UEs) depends on the infrastructure facilities provided by the service provider. In many cases service provider facilities functions like device discovery, authentication, spectrum allocation and service provider generate revenue from this. This is synonym with normal communication in cellular networks, spectrum used for the communication is licensed spectrum.
- **Partial Coverage:** In this scenario one of the UEs is facilitating D2D communication, by relaying cellular communication. This is typical use case of extending the coverage.
- **Out of Coverage:** In this scenario User Equipment (UEs) depends on the infrastructure facilities provided by the service provider. In many cases service provider facilities functions.

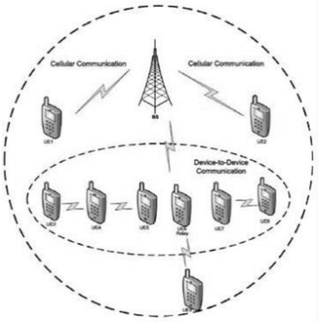

Fig. 3: Cellular and D2D Communication [15]

D2D communication scenario, enables merging of two key tech-nologies such as, ad hoc and centralized networking. D2D commu-nication operating in ad hoc network mode can benefit the service provider, can work in conjunction with other technologies like cooperative communication, cognitive radio, Internet of Things (IoT). This approach helps the service providers to enhance the spectral efficiency. On the other hand, with centralized networking, D2D communication helps in overall enhancement of the network performance, having the control from the operator [2].

Security requirements vary depending upon the use cases. As dis-cussed earlier, typical D2D communication can fall under any one of these categories, such as full coverage, partial or out of coverage. As discussed earlier, typical UE's will have two radio links, one will be used for cellular communication and second link will be used for D2D communication.

III. LIGHTWEIGHT CRYPTOGRAPHY

In recent days, Lightweight Cryptography is gaining lot of attention, this technology can play very important role for providing security for the communication devices which lacks computing power, to name few Internet of Things (IoT), Wireless Sensor Networks (WSN). Interestingly, Lightweight Cryptography is a branch of modern cryptography encompasses cryptographic algorithms, which are targeted for resource constrained devices. Sometimes this sounds like, "Lightweight Cryptography targeted for the systems with not so high security requirements", but, Lightweight Cryptography is equally needed for systems with high security requirements. As discussed in [16] National Institute of Standards and Technology (NIST) is statutorily responsible for developing standards (Federal Information Processing Standards or FIPS) and guidelines for the protection of information. NIST-approved cryptographic standards were designed to perform well on general-purpose computers. In recent years, there has been increased deployment of small computing devices that have limited resources with which to implement cryptography. When current NIST-approved algorithms can be engineered to fit into the limited resources of constrained environments, their performance may not be acceptable. For these reasons, NIST started a lightweight cryptography project that was tasked with learning more about the issues and developing a strategy for the standardization of lightweight crypto-graphic algorithms. In [17] comprehensive study of hardware implementation of some block ciphers which falls under the category of lightweight cryptography, such as SIMON, SPECK, PRESENT, KHUDRA and AES is carried out. This work covers mostly performance parameters such as throughput and power consumption of end devices. Also, security against cryptanalysis and side-channel security is discussed in detail. Essence of this work is different crypto-algorithms have different overheads with respect to counter measures used to defend against side-channel and cryptanalysis attacks. This work targets resource-constraints application, hence, can be applied for securing D2D communication. As we know Lightweight cryptography covers wide spectrum in terms of target devices and applications. Lightweight cryptography can be applied on devices with low hardware and memory capacity. Conventional cryptography can be applied on powerful computers, servers and smart phones. To identify the security requirements of resource constrained devices, Profile development is an important task, which is based on series of questions that needs to be answered. This will serve as a starting point for understanding of applications, identifying key bottlenecks if any, and helps in identifying additional constrains which may not be apparent at this point of time. The performance benefits of lightweight block ciphers over conventional block ciphers are achieved using lightweight design choices, such as, Smaller Block Sizes, Smaller Key Sizes, Simpler Rounds, Lightweight Message Authentication Codes [16].

As proposed in [21] the striking the right balance between stringent security requirement and resource constraint can be achieved by adopting approaches like using lesser block size and key length, choosing low-cost implementation but effective elements such as data dependent bit permutations and using operations that allow implementation trade-offs balancing resource available on the target platform.

As discussed in [22] in this era of Ubiquitous computing, there is a demand for crypto enabled and resource constrained devices. This demand in turn creates huge requirements for novel algorithms and cryptanalysis techniques. Hardware based Lightweight Crypto-graphic (LWC) algorithms measured based on number of logic gates used, approximately this count is up to 3000 logic gates. Hardware LWC implementations performance is comparable to traditional crypto-graphic techniques in terms of design complexity, power and energy consumption and throughput. Lightweight cryptography tries to achieve the required functionality with the minimum amount of hardware resources. Software implementation of LWC algorithms for resource constrained devices tries to keep CPU needs low in order to minimize power consumption.

As discussed in [23] Elliptic Curve Cryptography (ECC) is being considered for providing security to hand-held and mobile devices. ECC implementations uses shorter key length, also provides higher security on par with security provided RSA (Rivest-Shamir-Adleman) implementation. This advantage of ECC over RSA turns to be very attractive for mobile hand-held devices. ECC can also be used for securing D2D communication.

In [24] authors have presented analysis of various LWC implemen-tations. Comparing ECC with RSA, ECC is considered most attrac-tive for resource constrained devices because of its smaller operand lengths and relatively lower computational requirements. In [28] authors presented how ECC can be used for efficient key exchange between the end points. Elliptic Curve Cryptography can also be used authenticating the end points in terms of digital signature. In this case, the requirement is to choose the right Elliptic Curve to provide better performance and desired level of security based on the mobile and handheld device requirements. This work can be extended by choosing right curves for different Voice Over Internet Protocol (VOIP) end points and analysing the performance. This shows that ECC can be also be used in D2D communication. Such an approach would be considered as good as applying lightweight cryptography.

IV. SECURITY IN D2D COMMUNICATION

Existing surveys on Securing D2D communication focused on applying Mobile Ad-hock Network security techniques. There are similarities between D2D communication in out of coverage sce-nario and MANET, at the same time D2D communication co-exist with cellular communication in terms of full coverage and partial coverage scenarios. Security is very important in D2D Communi-cation. Common Security requirements of any wireless communi-cation includes but not limited to Authentication, Data Confidenti-ality, Data Integrity, Privacy, Non-repudiation, Privacy, Availability, Access Control. As we know, by nature Wireless communication is prone to different types of attacks. As discussed in [32] we can think of different attack scenarios, these attack modes are shown in Fig. 4. attacks can be classified into Eavesdropping attack, Impersonation attack, Message modification attack, Man-in-the-middle (MITM) attack and Denial of Service (DoS) attack. eavesdropping attack or passive listening can easily be achieved by running a sniffing soft-ware. All unencrypted data can be sniffed by an advisory. Impersonating attack can be launched by spoofing link layer and network layer address. In case of message modification attack, an advisory will sniff the traffic and modify the message by crafting packets and injecting them into the network. Man-in-the-middle or MITM is a well know attack in the wireless network where an advisory establishes independent connections with sender and receiver. After establishing such connections, attacker will modify the original communication between sender and receiver. One possible defence against such attack is to implement mutual authentication of sender and receiver. Denial of Service (DoS) attack can be severe, where an attacker consumes all the resources for example, establish maximum number of TCP connection with the target webserver so that after reaching the limit webserver will deny connections even to the legitimate users.

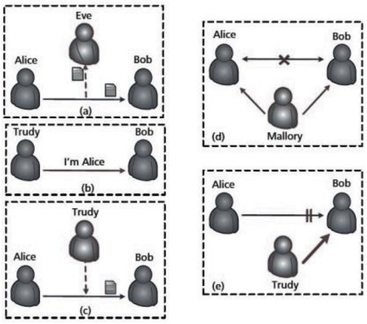

Fig.1: Attack modes: a) Eavesdropping; b) Impersonation; c) Message modification; d) MITM; e) DoS attack[32]

In [3] parameters used were UE latency and average relevant throughput. PKI based techniques used for providing the security, traffic offloading is the typical application scenario. Novel approach of gaming theory for clusterisation is used for creating cluster. This work mainly focuses on group communication. Simulation results shows that exploiting D2D connections leads to an increased throughput for the users at cost of an additional delay and energy consumption due to the signalling message exchange locally in the cluster. Even though it covers all 3 scenarios, lightweight cryptographic approach is not considered. Simulation done

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

In [4] authors proposed social-aware approach for optimizing D2D communication by exploiting social network layer and physical wireless network layer. Even though this work focuses Content sharing based on novel approach by using Indian Buffet Process. Simulation results shows that by using proposed algorithm data rate of the system has been increased. In this work only, privacy issue was dealt by providing incentive for the users to share the content. Authors claim that, proposed system closely resembles the real scenario. Proposed system considers in-band D2D communication, where most of the security issues will be handled by the service provider. However, there is a need to consider D2D outband communication scenarios. Lightweight cryptology techniques were not given consideration.

In [5] authors focused on out-of-coverage scenario, in which UEs form D2D networks in autonomous manner without supervision of any LTE infrastructure. Purpose and application scenario of this work is Public Safety and based on probabilistic key Management scheme. In this work authors borrowed the idea of random key pre-distribution among UEs from sensor networks, also used light-weight cryptographic technique, such as lightweight key exchange mechanism in creation of D2D network. Simulation results (network connectivity analysis) of proposed secure protocol shows that the existence of trade-off points between connectivity and the increased overhead added by security for different values of the system parameter. However, this research covers only subset of a bigger problem, in terms of coverage and techniques. Simulation done, implementation not done.

In [6] authors focus on extending PKI to partial coverage scenarios when Infrastructure becomes un-available. This work is more related to group communication and handles the scenario of admission of new UE into the group. When infrastructure is not available UEs uses D2D link for communication otherwise LTE link will be used. Main contribution of this work is authors proposed a novel security algorithm, which allows a group of devices that have initialized their D2D connection to be controlled and managed by the cellular network. The respective functionality includes adding new users to the secure coalition as well as excluding existing users from it, even in cases when the reliable cellular network connection is presently not available. However, there is no implementation or simulation of the proposed algorithm.

In [7] authors target secure key exchange in D2D scenario. In this work authors have considered only D2D communication out-of-coverage scenario. Focus area of this work is Authentication and Key agreement. As we know Diffie-Hellman key exchange is vul-nerable to Man-in-the-middle attack. In this work authors have implemented secure key exchange scheme by integrating this into existing Wi-Fi Direct protocol.

In [8] authors have not covered typical D2D scenarios like partial covered or full coverage scenarios, however focus is on ad-hoc mode, this work is mainly on mobile multiloop network, which is similar to D2D communication in out-of-coverage scenario. One main difference here is D2D communication could be one-hop communication whereas mobile communication in ad-hoc mode may involve multi-hop communication. However, in this work authors have covered Device-to-specific device in a group and Device-to-group communication. Cipher text Policy-Attribute Based Encryption and Bluetooth Authentication protocol has been implemented. This work has taken possible Man-in-the-Middle attack, Replay attack and Collusion attacks as security requirements and Communication cost, Storage cost and Computation cost as the parameter to measure efficiency of their implementation. Results shows that time taken for encryption increases with increase in number of attributes used in CP-ABE encryption. It is interesting factor that time required for decryption depends on the complexity of access policy rather than the number of attributes.

In this work authors proposed a scheme which is based on the Bluetooth protocol, this scheme resolve the initial key establishment and integrity problems in the presence of inside adversaries in multi-hop networks and can be extended to other D2D protocols such as Wi-Fi Direct. However, analysis shows that CP-ABE incurs relatively high cost. This is because it is done once and for a during the initial authentication procedure for the secure PIN delivery, also this covers only authentication part of the security requirement, at the same time one should think of providing security for the data in transit. Lightweight cryptographic techniques can be used for achieving this. Simulation is not done, Implementation of initial key establishment protocol on an Android smartphone is done using Java and the CP-ABE open source library.

In [9] Authors have considered the impacts of Denial of Service (DoS) attacks in a D2D underlaying network. Experimental results show that attacks can force UE to lose the Wi-Fi connection with the access point without being detected by the AP or the cellular network. The objective of this work was to investigate the effect of DoSattacks, this work covers in-coverage and ad-hoc mode com-munication scenarios. However, this work is having limited scope focusing only one attack and other aspects are ignored. Lightweight Cryptographic technique not considered here.

In [10] Authors presented a lightweight on-demand-puzzled IBE solution suitable for secure D2D discovery and communication. In this work authors also designed a protocol based on the modified IBE system to ensure privacy support and legal interception for D2D clients. This protocol is evaluated though a security analysis and is validated in a platform for a social network scenario using D2D aspect in single or multiple domains use cases. This work is related to addressing security issues in discovery and communica-tion phases, Scenarios covered are full coverage and UEs exist in single domain and full coverage but UEs in different domains Au-thors proposed hybrid solution that integrates IBE and ECC. Focus is key management in the scenarios where UEs belong to same operator and another scenario where UEs belong to different opera-tors.

In [11] Authors considered only full coverage scenario of D2D communication. This work is more on providing physical layer security, authors have adopted novel approach of D2D interference exploitation in D2D-enabled cellular networks, the interference generated by D2D communications can be exploited to enhance secure cellular communications and at the same time create extra transmission opportunities for D2D users. In nutshell, proposed model is based on D2D resource allocation scheme based on sto-chastic geometry. As rightly observed by the authors the main limitation of the proposed model is the communication mode of each user that is cellular mode or D2D mode is preset, but in practical situation this is not true, each user can change communication mode. Proposed model can resist Eavesdropping attack, but other attacks can be mounted. Lightweight cryptographic techniques are not explored in this work.

In [12] Authors proposed Security framework for proximity ser-vices, this work covers all 3 scenarios of D2D communication. Application scenario is extending the coverage and they have used game theory centric based clustering approach. Implementation is done using OpenSSL with RSA algorithm. Security system they have proposed is based on PKI technique and simulated their work using MATLAB. Experimental result shows that there is some amount of signaling overhead, but connectivity was provided, and performance parameters were good. In this work lightweight cryp-tographic techniques were not used.

In [13] Authors had investigated access control for D2D communi-cationunderlaying cellular network. Network Calculus theory is being used and proposed model facilitates interference avoidance between D2D and Cellular communication. Proposed system em-ploys multi-priority model which assigns strictly highest priority for cellular users and multiple levels of priority for D2D users in a single cell. Numerical simulation of proposed system shows that Quality of Service (QoS) of cellular system enhanced, however low priority D2D user’s communication is impacted not only by the cellular users but also by higher priority D2D users. Access control is one of the security requirements but at the same time other security requirements like authentication, authorization, data confidentiality, data integrity could have been considered. Light-weight cryptographic technique plays very important role, which is not considered in this work.

In [14] Authors presented work which focuses on secure group key agreement and routing. This work relays on PKI based authentica-tion. However lightweight cryptographic techniques were not con-sidered. Simulation results shows that proposed algorithm can be applied to the ad hoc D2D networks having up to 64 ad hoc nodes.

In [18] Authors have done extensive survey of Security in D2D communications. The entire work is based on classification of D2D communication in layered approach. D2D communication security requirements have been identified for each layer namely, Application layer, Network layer, Media Access layer and Physical layer. Contribution of existing work in this area by various researchers is mapped to these security requirements at each layer is compared against few identified parameters, operational mode (Network assisted mode, Adhoc mode), purpose, scenario and applications. This work provides guidelines for the future research. However, lightweight cryptographic techniques were not considered while comparing the existing work.

In [19] Authors work covers full coverage scenario, have proposed 3 protocols for authentication of UEs. Use case scenario is Traffic offloading and Social Networking. Traffic offloading scenario network detects 2 UE's are connected to the same eNodeB, applica-tion does not require D2D link, but network makes use of this sce-nario to reduce the load on access and core network by ensuring D2D link used for this scenario However in Social Networking scenario, applications in each device requires a D2D link between them, social networking application in UE1 discovers the target UE is in proximity, after such discovery D2D link between these 2 UEs is established. All 3 protocols proposed two types of channel are used for processing the key exchange. Public wireless channel which is insecure channel through which public keys are exchanged, even advisory can get the public keys, susceptible to MITM attack, Encrypted Dedicated channel similar to public channel but data is encrypted before sending through this channel, adversaries will not have access. Simulation is done using MATLAB results are compared with existing two protocols SeDS: Secure Data sharing Strategy and SeCD. Simulation results shows that communication overhead increases in protocol-3 due to dependency of eNodeB which generates and compares Keys. However, this work does not focus on use of lightweight cryptographic techniques, also does not cover partial coverage and no coverage scenarios.

In [20] Authors proposed security scoring using legitimacy patterns for measuring the security and compare security-scoring results from static and random allocation of legitimacy patterns. Simulation results shows that when the attack is carried out for longer duration, shorter legitimacy pattern is needed to detect the attack. This approach uses combination of encryption, authentication, secure routing and forwarding and prevention of virus, worms and malicious code. This work uses lightweight cryptographic technique, Security Scoring helps detecting attacks at the physical layer without requiring intensive computation. Using SeS, attacks are detected efficiently at the physical layer without requiring intensive computations at higher layers of the software stack. In addition, implementing security at the physical layer will complement the security of upper layers of the protocol stack, improve the overall system security and enable new responses to attack.

In [25] Authors considered physical-layer security, formulated radio resource allocation as a matching problem in a weighted bipartite graph. Simulation results show that the system secrecy capacity can be greatly improved by introducing D2D communications underlaying cellular networks. However, in this work, lightweight cryptographic techniques are not considered.

In [26] authors compared the physical layer security offered by a direct D2D connection between two network nodes. Expressions for the secrecy outage probability were derived. Simulation results shows that D2D mode offers a security advantage over decode-and-forward messaging through the Access Point. However lightweight cryptography is not considered.

In [27] authors have proposed secure message delivery protocol to securely deliver message for multi-hop D2D communication. In this work D2D communication full coverage and D2D communication partial coverage scenarios are not covered, only out of coverage scenario is covered. However, in this work, authors have not considered applying lightweight cryptographic techniques for providing security for D2D communication.

In [30] authors have proposed crypto system based on Elliptic curve and ElGamal over public-key infrastructure (EEoP). EEoP uses ECC for creation of keys and uses ElGamal for encryption and decryption over public-key infrastructure. The proposed system can be used in partial coverage scenario of D2D communication, also computationally lightweight. EEoP ensures the confidentiality and integrity of the communication.

In [31] authors have proposed a fast secret key extraction (KEEP) protocol to establish secure secret key between two communication entities. KEEP uses a validation recombination mechanism to obtain consistent secret keys from Channel State Information (CSI) measurements of all subcarriers available from Orthogonal Fre-quency-Division Multiplexing (OFDM). It achieves high security level of the keys and fast key-generation rate. Simulation results shows that KEEP achieves high security level against various attacks such as eavesdropping and predictable channel attack. However, this work considers only full coverage scenario of D2D communication and application of lightweight cryptographic techniques are not give due consideration.

In [32] authors have explored Wi-Fi Direct as the promising proto-col for providing security in D2D communication. Authors have identified security challenges in wireless communication, proposed a short authentication-string-based key agreement protocol, further they have integrated this SAS-based key agreement protocol into the existing Wi-Fi Direct protocol and implantation is done using Android smartphones. However, this is not complete solution. We have challenges in Wi-Fi Direct technology, such as slower data transfer rate, less energy efficient, compatibility issues and security related issues. Wi-Fi Direct uses the WPA security and certification protocols to establish and maintain a secure connection. attackers can access the Wi-Fi network and WLAN via the Wi-Fi Direct hardware of vulnerable enabled devices such as printers. Attackers can use the connection via Wi-Fi Direct to convince an enabled device to route from Wi-Fi to a local area network. Hence, there is a scope for using lightweight cryptographic techniques.

In [29] authors have presented a benchmarking framework for evaluating lightweight block ciphers which are widely used micro-controller platforms for IoT devices. However same thing can also be used for benchmarking lightweight block ciphers for D2D communication. This framework consists of metrics of interest such as Execution time, RAM footprint and Binary code size. We are hoping to use these metrics in our next work, while implementing lightweight block ciphers for securing D2D communication.

V. CONCLUSION

D2D communication is going to play very important role in near future. D2D communication can help in various scenarios like disaster recovery, emergency services. D2D communication is getting lot of attention 3GPP has already proposed proximity service which will be part of LTE-A.

Security is very important, however due to the very nature of D2D communication end devices need to communicate securely without using the infrastructure. Conventional cryptography might be good but not suitable for D2D communication. In such scenario's light-weight cryptography can be a good choice. In this paper we have analyzed current work on securing D2D communication. Most of the literature on D2D security confined to authentication of end user or devices. However, there is a need for providing security for data in transit. There are many open issues which can be investigated further, also there is huge scope for adopting lightweight cryptographic techniques which eventually enhance security and performance.

VI. ACKNOWLEDGEMENTS

This is a survey work related to my research domain. I would like to thank VTU Regional Research Center(RRC) Belagavi, Principal and Management of Cambridge Institute of Technology K.R Puram, Bangalore.

VII. APPENDIX

In this appendix, we provide comparison of current research work related to Securing D2D communication with application scenario, security considerations and use of lightweight cryptographic techniques.

Appendix
Comparative Analysis of Secure D2D Communication

Research Work	D2D Full Coverage	D2D Partial Coverage	D2D Out ofCoverage	Application Scenario	Security Considerations	LightweightCryptographic Techniques
[3]	Yes	Yes	Yes	GORUP communication	-	No
[4]	-	-	-	Social networking Media sharing (traffic offload)	Privacy	No
[5]	No	No	Yes	Public safety	Secrecy	Yes
[6]	Yes	Yes	Yes	Admission of new users into the group, PKI based secure group construction	-	No
[7]	No	No	Yes	Diffie-Hellman based key agreement	Secrecy	Yes
[8]	No	No	No	Multihop Communication in Adhoc mode, Cipher text Policy- Attribute Based Encryption	Authentication	No
[9]	Yes	No	No	Impacts of Denial-of-Service (DoS) attacks in a D2D underlaying network	-	Yes
[10]	Yes	No	No	UE's exists in single domain, ECC and Indentity Based Encryption Techniques	Privacy	Yes
[11]	Yes	No	No	Physical layer security, using interference exploitation techniques in D2D-enabled cellular networks,	Eavesdropping	No
[12]	Yes	Yes	Yes	OpenSSL with RSA, extending the coverage using Game theory based Clustering approach	-	No
[13]	-	-	-	Multi priority model, Network Calclus theory	-	No
[14]	Yes	Yes	Yes	PKI based Group Key Agreement and routing, offload local traffic	Authentication	No
[19]	Yes	No	No	Man-in-the-Middle attack, Secure Key Exchange Traffic Offload, Social Networking	Authentication	No
[20]	-	-	-	Contineous authenticity using Security-scoring using legitimacy pattern	-	Yes
[25]	-	-	-	System scecracy capacity	Secrecy	No
[26]	-	-	-	Security provided at Physical layer	Eavesdrop	No
[27]	-	-	Yes	Secure path to deliver the message	-	No
[30]	No	Yes	No	Man-in-the-Middle attack, Secure Key Exchange	Secrecy, Integrity	Yes
[31]	Yes	No	No	Secure Key Exchange	Eavesdropping,Secrecy	No
[32]	Yes	Yes	Yes	Secure Key Exchange	Secrecy	No

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

REFERENCES

1. A. Asadi, Q. Wang and V. Mancuso, "A Survey on Device-to-Device Communication in Cellular Networks," in *IEEE Communications Surveys & Tutorials*, Vol. 16, No. 4, (2014), pp. 1801-1819, http://dx.doi.org/10.1109/COMST.2014.2319555
2. PimmyGandotra, Rakesh Kumar Jha and Sanjeev Jain, "A Survey on Device-to-Device (D2D) Communication: Architecture and Security Issues," *Journal of Network and Computer Applications*, Vol. 78, (2017), pp. 9-29, http://dx.doi.org/ 10.1016/ j.jnca.2016.11.002
3. A. Orsino and A. Ometov, "Validating Information Security Framework for Offloading from LTE onto D2D Links," in *Proceedings of the 18th Conference of Open Innovation and Seminar on Information Technology (FRUCT-ISPIT)*, (2016), pp. 241-247, http://dx.doi.org/10.1109/FRUCT-ISPIT.2016.7561534
4. Y. Zhang, E. Pan, L. Song, W. Saad, and Z. Dawy, "Social Network Aware Device-to-Device Communication in Wireless Networks," in *IEEE Transactions on Wireless Communications*, Vol. 14, No.1,(2015), pp.177-190, http://dx.doi.org/10.1109/ TWC.2014.2334661
5. L. Goratti, G. Steri, K. Gomez, and G. Baldini, "Connectivity and security in a D2D communication protocol for public safety applications," *International Symposium on Wireless Communications Systems (ISWCS)*, (2014), pp. 548-552, http://dx.doi.org/10.1109/ ISWCS.2014.6933414
6. AleksandrOmetov, Konstantin Zhidanov, Sergey Bezzateev, Roman Florea, Sergey Andreev and YevgeniKoucheryavy, "Securing Network-Assisted Direct Communication: The Case of Unreliable Cellular Connectivity," in *Proceedings of IEEE 14th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), (2015), pp. 826-833,* http://dx.doi.org/10.1109/Trustcom.2015.453
7. W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila and Y. Cheng, "Secure key establishment for Device-to-Device communications," *IEEE Global Communications Conference,(GLOBECOM)*, (2014), pp. 336-340, http://dx.doi.org/ 10.1109/GLOCOM.2014.7036830
8. Kwon, H., Kim, D., Hahn, C. et al, "Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks", *Multimedia Tools and Applications*, Vol. 76, Issue 19, pp.19507–19521, (2017), http://dx.doi.org/10.1007/s11042-015-3187-z
9. A. Hadiks, Y. Chen, F. Li and B. Liu, " A study of stealthy denial-of-service attacks in Wi-Fi direct device-to-device networks," in *IEEE 11th Consumer Communications and Networking Conference (CCNC)*, (2014), pp. 507-508, http://dx.doi.org/ 10.1109/ CCNC.2014.6994425
10. E. Abd-Elrahman, H. Ibn-khedher, H. Afifi and T. Toukabri, "Fast group discovery and non-repudiation in D2D communications using IBE", *International Wireless Communications and Mobile Computing Conference (IWCMC)*, (2015), pp.616-621, http://dx.doi.org/ 10.1109/IWCMC.2015.7289154
11. C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui and X. Wang, "Interference Exploitation in D2D-Enabled Cellular Networks: A Secrecy Perspective", in *IEEE Transactions on Communications*, (2015), Vol. 63, No. 1, pp. 229-242, http://dx.doi.org/ 10.1109/ TCOMM.2014.2379633
12. A. Ometov, A. Orsino, L. Militano, G. Araniti, D. Moltchanov and S. Andreev, "A Novel Security-Centric Framework for D2D Connectivity Based on Spatial and Social Proximity," *Computer Networks*, (2016), Vol. 107, Part 2, pp. 327-338, https://doi.org/ 10.1016/j.comnet.2016.03.013
13. Huang, Jun, Yi Sun, ZiXiong, QiangDuan, Yanxiao Zhao, Xianghui Cao, and Wei Wang, "Modeling and Analysis on Access Control for Device-to-Device Communications in Cellular Network: A Network-Calculus-Based Approach," in *IEEE Transactions on Vehicular Technology*, (2016), Vol. 65, No. 3, pp. 1615-1626, https://doi.org/ 10.1109/TVT.2015.2412154
14. Younchan Jung, Enrique Festijo, MarnelPeradilla, "Joint operation of routing control and group key management for 5G ad hoc D2D networks" International Conference on Privacy and Security in Mobile Systems (PRISMS), (2014), pp. 1-8, https://doi.org/10.1109/ PRISMS.2014.6970602
15. UditNarayanaKar and Debarshi Kumar Sanyal, "An Overview of Device-to-device Communication in Cellular Networks", *ICT Express*, (2017), https://doi.org/10.1016/j.icte.2017.08.002.
16. Kerry A. McKay, Larry Bassham, MeltemSönmezTuran, Nicky Mouha, "Report on Lightweight Cryptography", *National Institute of Standards and Technology Internal Report 8114*, (2017), https://doi.org/10.6028/NIST.IR.8114
17. Sadhukhan, R., Patranabis, S., Ghoshal, A. et al., *Journal of Hardware and Systems Security*, (2017), Vol. 1, Issue 3, pp 203–218, https://dx.doi.org/10.1007/s41635-017-0021-2
18. OthmaneNaitHamoud, TayebKenaza and YacineChallal, "Security in device-to-device communications: a survey," in *IET Networks*, (2018), Vol. 7, No. 1, pp. 14-22, http://dx.doi.org/10.1049/iet-net.2017.0119
19. RavindranathSedidi and Abhinav Kumar, "Key exchange protocols for secure Device-to-Device (D2D) communication in 5G," *The Wireless Days Conference*, (2016), pp. 1-6, http://dx.doi.org/10.1109/ WD.2016.7461477
20. I. Abualhaol and S. Muegge, "Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns," *49th Hawaii International Conference on System Sciences (HICSS)*, (2016), pp. 5763-5771, http://dx.doi.org/10.1109/HICSS.2016.713
21. Panasenko, Sergey P. and Sergey A. Smagin, "Lightweight Cryptography: Underlying Principles and Approaches", *International Journal of Computer Theory and Engineering*, (2011), Vol. 3, No. 4, available online: http://www.ijcte.org/show-37-375-1.html, last visit:01.11.2018
22. Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. et al.,"A review of lightweight block ciphers", *Journal of Cryptographic Engineering*, (2018),Vol. 8, Issue 2, pp 141–184, https://doi.org/10.1007/s13389-017-0160-y
23. Ajithkumar V and K Satyanarayan Reddy, "A Survey on Security of Mobile Handheld devices through Elliptic Curve Cryptography", ACCENTS Transactions on Information Security, (2017), Vol.2, No.6, pp.32-35, http://dx.doi.org/10.19101/TIS.2017.26001
24. T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann and L. Uhsadel, "A Survey of Lightweight-Cryptography Implementations," in *IEEE Design & Test of Computers*, (2007), Vol. 24, No. 6, pp. 522-533, http://dx.doi.org/10.1109/MDT.2007.178
25. H. Zhang, T. Wang, L. Song and Z. Han, "Radio resource allocation for physical-layer security in D2D underlay communications", *IEEE International Conference on Communications (ICC)*, (2014), pp.2319-2324, http://dx.doi.org/10.1109/ICC.2014.6883669
26. D. Zhu, A et al., "Device-to-device communications: The physical layer security advantage", *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, (2014), 2014, pp. 1606-1610. http://dx.doi.org/ 10.1109/ICASSP.2014.6853869
27. E. Panaousis, T. Alpcan, H. Fereidooni, and M. Conti, "Secure message delivery games for Device-to-Device communications," *Decision and Game Theory for Security, Lecture Notes in Computer Science*,(2014), Vol.8840, pp. 195-215.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

28. AjithkumarVyasarao and K Satyanarayan Reddy, "Application of Elliptic Curve Cryptography for Mobile and Handheld devices", in *Proceedings of International Conference on Contemporary Issues of Science, Engineering and Management (ICCI-SEM-2K17)*, (2017), pp. 87-91, ISBN:978-93-86352-38-5
29. Dinu, D., Corre, Y.L., Khovratovich, D. et al., "Triathlon of lightweight block ciphers for the Internet of things*", Journal of Cryptographic Engineering*, (2018), pp.1-20, http://dx.doi.org/ 10.1007/s13389-018-0193-x
30. YasirJaved, Adnan Shahid Khan, Abdul QaharandJohari Abdullah, "EEoP: A Lightweight Security Scheme over PKI in D2D Cellular Networks", *Journal of Telecommunication Electronic and Computer Engineering*, (2018), Vol. 9, No. 3-11, pp 99-105.
31. M. JanardhanaRajuRaju, Dr. P.Subbaiah, V.Ramesh, "A Novel Elliptic Curve Cryptography Based AODV for Mobile Ad-Hoc Networks for Enhanced Security", Journal of Theoretical and Applied Information Technology, Vol.58, Issue 3, Dec'2013.
32. Wei Xi et al., "KEEP: Fast secret key extraction protocol for D2D communication", *IEEE 22nd International Symposium of Quality of Service (IWQoS),* (2014), pp. 350-359, http//dx.doi.org/10.1109/ IWQoS.2014.6914340
33. W. Shen, B. Yin, X. Cao, L. X. Cai and Y. Cheng, "Secure device-to-device communications over WiFi direct," in *IEEE Network*, (2016), Vol. 30, No. 5, pp. 4-9, http://dx.doi.org/10.1109/ MNET.2016.7579020

Ajith Kumar. V is currently a Ph.D. student at Visvesvaraya Technological University, Regional Research Center of Belagavi. His research focus is on security for resource-constrained devices and application of lightweight cryptographic techniques for securing D2D communication. He obtained B.Sc. degree from University of Mysore in 1991 and his M.C.A., degree from Kuvempu University in 1999. His interest includes Computer Forensics, Cyber Security. He is life member of Cryptology Research Society of India (CRSI).

Dr. K. Satyanarayan Reddy. His qualification includes Ph.D. in Computer Science (Dravidian University, Kuppam, AP), MTech in Computer Applications (Dept. Of CSE, ISM Dhanbad). He has worked as faculty in many Engineering Colleges ,currently he is associated with Dept. of CSE, Cambridge Institute of Technology, Bangalore. He has more than 25 Research Papers (National and International) in his credit and has chaired national and international conferences. Delivered Keynote address in few national level conferences.