International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

A Survey on Bio-Inspired Proximity Discovery and Synchronization with Security Solutions for D2D Communications

Abhijeet Dholeshwar, Prof. Deepali Salapurkar

[1]*PG Student, Dept. of Computer Engineering, Sinhgad College of Engineering, Pune, Maharashtra, India*
[2] *Assistant Professor, Dept. of Computer Engineering, Sinhgad College of Engineering, Pune, Maharashtra, India*

Abstract - *Device-to-Device (D2D) Communication is a fast emerging technology in recent years. It serves an end to end communication without depending upon any infrastructure. Various proximity models are present to identify and communicate with the different devices present in the vicinity of a particular device. In these services security should also be concerned as it is the least dealt area of D2D communication. In this work, a distributed mechanism for application aware Proximity Services (ProSe) in D2D communication is proposed. This method is a derivation of bio-inspired firefly algorithm which can achieve proximity discovery and synchronization at same time. The basic firefly algorithm has limitation for large scale system such as LTE-A D2D, which has been covered in the derived algorithm by enabling simultaneous neighbor discovery and service discovery as well as synchronization in physical communication timing. The existing security mechanisms are reused with some modifications, providing potential solutions which are based on various security architectures and requirements. Authentication and key management solutions are proposed according to various scenarios.*

Key Words: D2D communication; ProSe; LTE

1. INTRODUCTION

Device to Device (D2D) communication is gaining importance with a notable increase in wireless technologies and devices; and their usage. Due to such type of communication, our wireless devices such as mobile phones, tablets etc. could be used, even if no network infrastructure is present. It is helpful in certain scenario such as any disaster affected area where communications are destroyed. D2D communication can be achieved efficiently with the help of certain parameters such as neighbour discovery, message passing, connectivity etc. D2D communication can give better resource utilization and higher data transmissions in networks.

The Third Generation Partnership Project (3GPP) Long Term Evolution (LTE) has launched D2D applications in such cases which require direct access with and without infrastructure. In infrastructure based D2D communication, initiation of device to device communication is managed by Base Station (BS). User Equipment (UE) searches its neighbour and transmits data in the proximity in self-organized manner, without assistance from BS. Two devices will communicate when they fulfil each others' criteria of proximity. The main required criterion of proximity is geographical distance between devices. Proximity Service (i.e. ProSe) is defined in proximity context and it is an important feature of D2D communications. ProSe consist discovery of devices and communication among these devices which are in close physical context.

The proximity discovery can be categorized in two contexts; physical communication and application discovery. In physical level proximity discovery, signal exchange among devices takes place whereas in application level discovery a device search another device having same applicability in the network. To make communication among devices durable and efficient, there is need to merge the physical communication with application discovery.

From security point of view, we can classify the various scenarios of ProSe, mainly in three categories as illustrated in Fig. 1

- Type 1 scenario: network-covered D2D without user apps
  - All devices in proximity are covered by LTE-A networks without user applications
- Type 2 scenario: network-covered D2D with user apps
  - All devices in proximity are covered by LTE-A networks with certain user apps.
- Type 3 scenario: network-absent D2D for public safety
  - At least one device in proximity is not covered by LTE-A networks.

Only Type 3 scenario related work is taken into account due to its applicability in disaster situation. A disaster affected area needs emergency help and attention. But due to the calamity the communication means may go down. At sch scenario D2D Communication could be helpful.

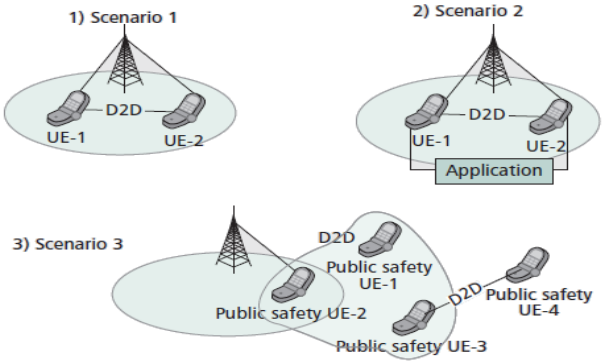

Fig -1: Types of D2D Scenario

2. LITERATURE REVIEW

Bio-inspired computing is a field of study that cleverly binds subfields related to the topics of connectionism, social behavior and emergence. It relies heavily on the fields of biology, computer science and mathematics. It efficiently uses models present in real life which are practiced by living organisms such as insects etc. It is the use of computers to model the living phenomena, and the study of life to improve the usage of computers.

In [5], a model of population of identical integrate-and-fire oscillators is studied. The coupling between oscillators is pulsatile: when a given oscillator fires, it pulls the others up by a fixed amount, or brings them to the firing threshold, whichever is less. The main result is that for almost all initial conditions, the population evolves to a state in which all the oscillators are firing synchronously.

In [16], Wener-Allen et al. implemented decentralized Reachback Firefly Algorithm (i.e. RFA) on TinyOS-based motes and provided theoretical improved result. This algorithm is based on a mathematical model that describes how fireflies and neurons spontaneously synchronize. This algorithm accounts for realistic effects of sensor networks by allowing nodes to use delayed information from the past to adjust the future firing phase.

Authors [17] proposed Meshed Emergent Firefly Synchronization (i.e. MEMFIS) which multiplexes synchronization word with data packet and adopt local clock upon reception of synchronizing nodes. A dedicated synchronization phase is mitigated, as a network-wide slot structure emerges seamlessly over time as nodes exchange data packets.

In [18], authors applied firefly model for synchronizing ad hoc networks. They had used a phenomenon that Fireflies exhibit a fascinating phenomenon of spontaneous synchronization that occurs in nature: at dawn, they gather on trees and synchronize progressively without relying on a central entity.

Authors [19] discussed about the general model of synchronization and convergent condition of nodes in network. A class of synchronization protocols for dense, large-scale sensor networks is presented. A class of models is presented that converge to a synchronized state based on the local communication topology of the sensor network.

Table -1: Comparative Analysis

Sr	Technique/Idea	Description	Drawback
1.	Firefly Algorithm[1]	Proximity Discovery and Synchronization is done simultaneously using FST	Nos. of message exchanges increase overhead increase.
2.	ProSe Overview [3]	How D2D proximity services should be designed according to the principles and scenario	Standards not necessarily applied over enhanced D2D devices.
3.	Reachback Firefly Algorithm [16]	RFA Algorithm used for effective synchronization	Difference in topology parameters not given.
4.	Authentication and Key management mechanisms [6]	Overview of existing security models and possible solutions on security problems.	Social networking security mechanism not covered.

3. FIREFLY ALGORITHM

This algorithm is inspired by the fireflies and the synchronization between the swarm of fireflies. Fireflies use its flash, which flashes at certain threshold interval, and locate other fireflies by recording their flashes and also gives its own status. Thus each firefly gets synchronized in the swarm.

The similar model can be used by the UEs to achieve synchronization with an effective proximity discovery. The devices discover each other by sending signals and increasing the counter values. The flow diagram for Firefly algorithm is given in Figure 2. When the threshold is reached, proximate devices come into a synchronized network and start communicating. To reduce the extensive signaling processes in both physical and application levels of proximity discovery, the concept of firefly synchronization into D2D communications has been introduced. The properties of the algorithm are suitable to an idealized system such as a full meshed network. But a constant topology is not possible in real application. So achieving synchronization is a difficult task. This was the problem with firefly algorithm.

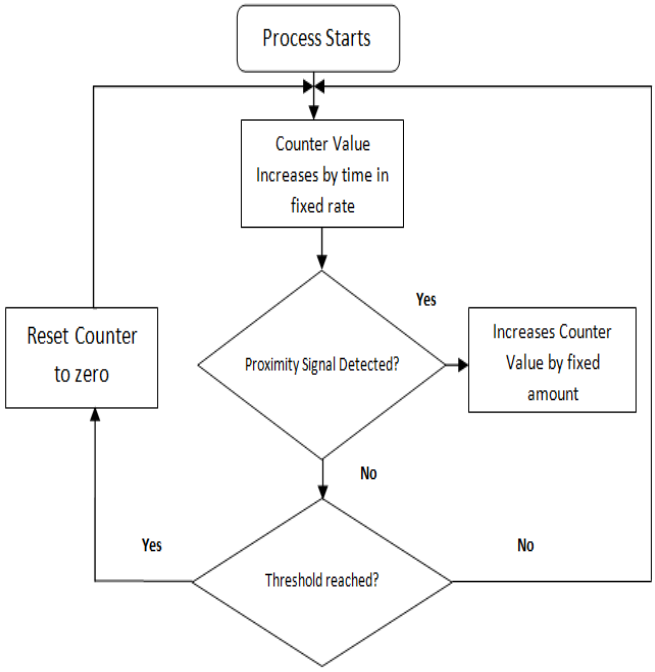

Fig -2: Firefly Algorithm Flowchart

4. FIREFLY SPANNING TREE

It is difficult to implement any similar method, for synchronization, on a randomly generated topology. Firefly Spanning Tree (FST) can provide a solution to it. FST includes forming a structure of heavy nodes; i.e. taking the nodes with better links; and establishing communication between them.

According to FST, a D2D network can be formulated into a graph G (V, E), where vertices V are independent UEs or devices and edges E are communication links between UEs. Links can be weighted using the strength of the Proximity Signal which is sent to discover proximate devices. The benefits of the mechanism, in any randomly generated topologies, can be reaped by finding a basic structure which is able to sustain the state of synchronization. Tree may be a suitable structure which will be helpful in synchronization. The theorem proving stability of tree is given in [1].

FST is a distributed algorithm which may construct a spanning tree with strongest signal strength on graph maintaining a distributed manner.

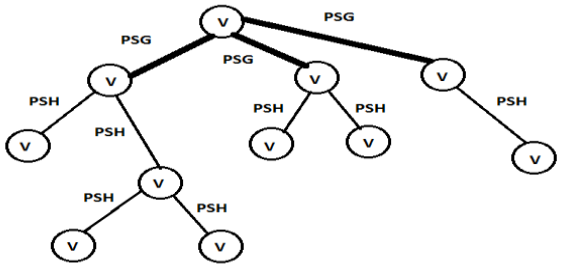

Fig -3: Illustration of Firefly Spanning Tree

5. PRE-SHARED-KEY BASED SECURITY SCHEME

It is difficult to implement any similar method, for synchronization, on a randomly generated topology. Firefly Spanning Tree (FST) can provide a solution to it. FST includes forming a structure of heavy nodes

5.1 Security Requirements

Before The three types of scenarios, as shown in Fig. 1, share the following security requirements in common:

- Reusing the existing LTE-A security architecture so as to reduce deployment costs
- Secure connection between ProSe function and other network elements in core networks
- Secure connection between UEs against any passive or active attacks

Type 2-scenarios have some additional requirements:

- Secure connection between ProSe application servers and networks as well as between servers and end-user applications
- To protect communication contents and user privacy, from leaking as side information during the communication

Type-3 scenarios do not have assistance from an LTE-A network, and have an enhanced requirement:

- In the absence of a network, the direct radio link should provide secure node discovery and authentication between UE devices.

5.2 Security Scheme

In type-3 scenario, security should be provided in node discovery and authentication phase. For this purpose, a hard-coded pre-distributed shared key can be helpful. Consider an example where a Disaster Rescue Team enters a disaster area where the main control node is destroyed. In such case, their specially-made public safety User Equipment allows them to set up direct communication with each other using LTE-A technologies and in a secure manner with the help of the pre-shared key. It enables them to connect to the nearest available network through other public safety UE in the network coverage as relay. Thus the pre-shared key can be used to connect only the legitimate people.

This scheme involves two levels of key exchanges which can give out two types of changes

- The first change is essential to protect against a record and replay attack, where an intruder records the information it hears and transmits it again later pretending to be the original sender.
- The second change allows every public safety UEi to set up a pair of broadcasting keys (Cipher Key CKi, Intermediate Key IKi) to communicate with all reachable users.
- If only two UE want to communicate with each other privately then they can use pair of pair-wise keys by XORing CK1 and CK2, IK1 and IK2

The scheme is as illustrated in Fig. 4

It uses pair of (CK, IK) and distributions of these keys with certain modifications at each stage are done. A Key Distribution Function (KDF) is responsible for key generation and distribution of it.

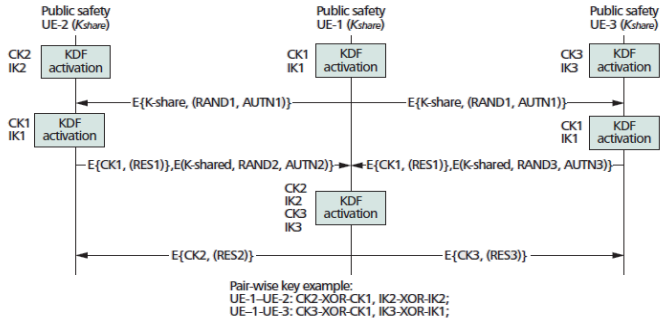

Figure -4: Pre-shared Key Based Security Scheme

6. METHODOLOGY

A well structured and synchronized network with security feature can be modular for D2D communication. Firefly Spanning Tree can keep the network well synchronized and Pre-shared Key based scheme can help in forming network with security. Both methods together can provide solution for a secure and structured network.

FST is a two-level algorithm. At the beginning, devices know only the weight of links which are connected to them. Later every device observes that which of its link belong to FST and synchronizes with remaining neighbors. The process involves two different proximity signals. PSH is used for the synchronization between sub-graphs. PSG is used for the regular operation of the basic firefly algorithm throughout the network. Illustration is shown in Figure 3.

The architecture of pre-shared key based security scheme is shown in Figure 4. The authentication scheme described above can be reused. The steps involved in this scheme are as follows

- Here it is assumed that there is a pre-distributed hard-coded shared key, K*share*.
- Consider a network of three users, where UE-1 is able to reach the other two UEs, while UE-2 and UE-3 can only communicate with UE-1 individually.
- The broadcast information of random number RAND and authentication token AUTN i.e. (RAND, AUTN) is encrypted using the shared key.
- The Response number RES is encrypted using the newly generated cipher Key, CK. UE-2 and UE-3 not only respond to the challenge posed by UE-1, but also broadcast their own vector (RAND, AUTN).
- UE-1 realizes the devices by this response and matches the credentials. If legitimate, it again encrypts this RES with newly generated cipher keys and sends to respective legitimate user.
- Newly formed pair keys are responsible for authenticate communication between the users.

If UE-1 and UE-2 want to privately communicate then XORing the pair of keys would be a solution for it without broadcasting to all the reachable users.

3. CONCLUSIONS

A well administered distributed mechanism for D2D network ProSe could be able to achieve proximity discovery and synchronization at same time. The mechanism could serve in both physical and application level. The problem of different topology may also be solved. The two features viz. the availability of a network and the presence of a user application could affect the management of the network, which results in different security requirements. The LTE-A D2D scenarios can be classified into three typical types based on these features. A Preshared-Key authentication and key management solution is proposed by reusing existing functions and algorithms for Type-3 scenario which will be helpful in disastrous situation.

REFERENCES

[1] Shih-Lung Chao, Hsin-Ying Lee, Ching-Chun Chou, and Hung-Yu Wei, “Bio-Inspired Proximity Discovery and Synchronization for D2D Communications”, IEEE Communication Letters, Accepted for Publication, 1089-7798/13M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[2] Klaus Doppler, Mika Rinne, Carl Wijting, Cssio B. Ribeiro, and Klaus Hugl, “Device-to-Device Communication as an Underlay to LTE-Advanced Networks, IEEE Communications Magazine”, Dec 2009.

[3] Xingqin Lin, Jeffrey G. Andrews, Amitabha Ghosh, and Rapeepat Ratasuk, ”An Overview of 3GPP Device to Device Proximity Services” , IEEE Communications Magazine, April 2014.

[4] Geoffrey WernerAllen, Geetika Tewari, Ankit Patel, Matt Welsh, Radhika Nagpal ,” Firefly Inspired Sensor Network Synchronicity with Realistic Radio Effects “, SenSys05, November 24, 2005, San Diego, California, USA. Copyright 2005 ACM 159593054X/ 05/0011.

[5] Renato E. Mirollo; Steven H. Strogatz , “Synchronization of Pulse-Coupled Biological Oscillators”, SIAM Journal on Applied Mathematics, Vol. 50, No. 6. (Dec., 1990), pp. 1645-1662.

[6] Muhammad Alam, Du Yang, Jonathan Rodriguez, and Raed A. Abd Alhameed, “Secure Device-to-Device Communication in LTE-A IEEE Communications Magazine , 0163-6804/14.

[7] Technical Report 22.803 v12.0.0, Feasibility study on proximity services (ProSe), 3GPP, 2012.

[8] K. Doppler, C. B. Ribeiro, and J. Kneckt, Advances in D2D communications: energy efficient service and device discovery radio, in Proc. 2011 Wireless VITAE, pp. 16.

[9] C. Mehlfhrer, J. Colom Ikuno, M. Simko, S. Schwarz, M. Wrulich, and M. Rupp,” The Vienna LTE simulators enabling reproducibility in wireless communications research”, EURASIP J. Advances Signal Process., vol. 2011, pp. 113, 2011.

[10] R. G. Gallager, P. A. Humblet, and P. M. Spira,” A distributed algorithm for minimum-weight spanning trees”, ACM Trans. Program. Lang. Syst., vol. 5, no. 1, pp. 6677, 1983.

[11] C. H. Rentel and T. Kunz, “Clock-sampling mutual network synchronization for mobile multi-hop wireless ad hoc networks”, in Proc. 2007 MILCOM

[12] G. Simon et al. “Sensor network-based countersniper system”. In Proc. ACM SenSys 04, Nov 2004.

[13] N. Wakamiya and M. Murata., “Scalable and robust scheme for data fusion in sensor networks”, In Intl Workshop on Biologically Inspired Approaches to Advanced Information Technology, Jan 2004.

[14] G. Werner-Allen, J. Johnson, M. Ruiz, J. Lees, and M. Welsh. “Monitoring volcanic eruptions with a wireless sensor network”, In Proc. European Workshop on Wireless Sensor Networks (EWSN05), Jan 2005.

[15] G. Werner-Allen, P. Swieskowski, and M. Welsh. "MoteLab: A wireless sensor network testbed", In Proc. IPSN05, Special Track on Platform Tools and Design Methods (SPOTS), April 2005.

[16] G. Werner-Allen, G. Tewari, A. Patel, M. Welsh, and R. Nagpal, "Firefly inspired sensor network synchronicity with realistic radio effects", in Proceedings of the 3rd international conference on Embedded networked sensor systems, pp. 142 153, ACM, 2005.

[17] A. Tyrrell, G. Auer, and C. Bettstetter, "Emergent slot synchronization in wireless networks", IEEE Transactions on Mobile Computing, vol. 9, no. 5, pp. 719732, 2010.

[18] A. Tyrrell, G. Auer, and C. Bettstetter, "Fireflies as role models for synchronization in ad hoc networks", in Proceedings of the 1st international conference on Bio inspired models of network, information and computing systems, p. 4, ACM, 2006.

[19] D. Lucarelli, I.-J. Wang, et al., "Decentralized synchronization protocols with nearest neighbor communication", in Proceedings of the 2nd international conference on Embedded networked sensor systems, pp. 6268, ACM, 2004.