A Study Of Bio-inspired Self Organizing Networks

Juniorika lyngdoh[1], Hemanta Kumar Kalita[2]

[1,2] Department of IT
North Eastern Hill University
Shillong, Meghalaya, India.
rikalyngdoh@gmail.com, kalita.hemanta@gmail.com

Abstract:*In today's perplexed world of wireless networking, there are many rapid changes and challenges that could lead to an excessive quantity of users flocking to one or only a few networks, thereby leaving some potentially subsidiary accommodation providers out of the picture. Self-Organizing Networks (SON) is a term for mobile network automation, cost efficient, easy operation and maintenance of mobile networks .This article provides an overview of SON features and challenges. Since self-organization is expected to bring us remarkable benefits in terms of costs reduction in network configuration, management, operation and optimization, etc, enormous research has been carried out to address the challenges brought by the ever increasing complexity and dynamics in complex communications systems.*

Keywords:SON; Self organizing networks

1. . Introduction

In the recent years we have noticed that there was an explosive growth of wireless telecommunication and networking. A wide variety of new technologies such as WIFI, bluetooth, zigbee, ultra-wideband communications, and long- term evolution (LTE) has been introduced to provide more consumer options. in the meantime, a lot of physical systems are cordlessly connected with the cyber infrastructure, as well as vehicle-to-vehicle (V2V) communications, smart power grid communications, machine-to-machine communications (M2M), and internet of things (IOT), resulting in complicated physical systems. All these developments with their rapid growth will be even more challenging. Without well thought-out management and coordination, a worst scenario could emerge, where the majority of users crowd a certain service network, while others are left underutilized [1]. Evidently, our traditional network structure designed with a designated signaling technique and limited number of users can no longer accommodate these emerging challenges. so, a new networking framework is needed that can adaptively self-organize regardless of the heterogeneity in communication devices, systems and applications, and at the same time scale to a vast number of users and remain robust against dynamic and possibly abrupt changes in the increasingly complex wireless environment. On the other hand, self-organizing networks (sons) are expected to enhance the utilization of radio re- sources by simplifying network management and reducing thecost of operation [2]. The hierarchical trend of son includes a number of general progressions to arrange the network, i.e. self- planning, self-configuration, self-optimization, self- operation and self-correction. Each of the mentioned procedures includes part of the novel features and matters within the proposed algorithm. While this greatly increased the number of users in the entire communication network leading to persistent communication and computing. So, a new networking frame- work is needed that can adaptively self-organize regardless of the heterogeneity in communication devices, systems and applications, and at the same time scale to a vast number of users and remain robust against dynamic and possibly abrupt changes in the increasingly complexwireless environment[3]. In self organization was defined as the emergence of system- wide adaptive structure and functionality from simple local interactions between individual entities. In some appealing self-organization characteristics, such as the ability to self-organize in a fully distributed fashion, collaboratively achieving efficient equilibrium, have been generalized from biological systems and processes. since self-organization is expected to bring benefits in terms of cost reduction in network, management, operation and optimization, etc, enormous research have been done to address the challenges and complexity, heterogeneity, and dynamics in complex communications systems. The study of collective behavior (or in other words, swarm intelligence) of social species can help humans manage complex systems, and bio-inspired algorithms have already given us some illumination on designing, maintaining and optimizing artificial son systems.

The phenomenon of self-organization is pervasive in many areas of life example like fish organize themselves to swim in well-structured swarms, ants find shortest routes to find food sources, and fireflies emit light flashes in a synchronized fashion. In all the above examples, the participating entities establish an organizational structure that does not require any central coordination. Instead, the entities interact directly with each other, reacting to changes in their local environment. Typically, such self-organizing systems are very flexible, adaptive, failure-robust, and scalable [4]. In this paper after a general introduction to SON, the fundamental features of SON are reviewed then the research challenges within SON domains were highlighted followed by the Bio inspired techniques to Network Security and finally the conclusion.

2. Fundamental features of self- organizing networks.

In existing literatures, more essential properties that regarded as fundamental SON mechanisms and principles have been summarized, such as [3][5].

• **Systematism**: Self organization is a system wide activity that can practice of classify or systematize coherent system that has parts of interactions, structural relationships, behavior, state, and a border that delimits it from its environment.

• **Complexity**: SON systems are complex which imply that there is self- organization and emergence in complex systems. Complex systems are organized in a distributed manner without centralized control. If one knows the parts of self-organized systems as well as the connections between those parts, it is still difficult to model the systems and to predict their behavior.

• **Cohesion**: The degree to which the elements of a component belong together. Thus, cohesion measures
the strength of relationship between pieces of functionality within a given component.

• **Non-linearity**: Self-organization is a process in which the higher-level components of the system emerges
Solely from numerous interactions among the lower- level components. The overall system can perform more powerful and complex tasks.

• **Distributed control**: In a distributed control mechanism no external component from outside of the
SON system is responsible for guiding, directing or controlling the system. Each individual works on its own intention.

• **Adaptively**: SON systems are capable of adapting to changing environments and being flexible to failures and damages.

3. Self-Organizing Network Areas.

The Self-X capabilities of Self organizing networks can be summarized as follows [8].

• Self-Configuration: The aim is they should need as little manual intervention in the configuration process as possible Self-configuration is a process with the newly deployed being configured by automatic installation procedures to get basic parameters and download necessary software for operation. Several self-configuration mechanisms have been proposed in wireless cellular networks. The initial configuration of network elements in a mobile network is complicated by a large number of parameters. Handling configuration manually is tedious and time consuming.

• Self-Optimization: enable a mobile network to adaptively optimize their algorithms and system parameters to achieve optimal system performance (in terms of, e.g., capacity, service coverage, etc.) in the presence of environment changes, are crucial for the operation and maintenance of mobile networks. Once the system has been set up, it will be necessary to optimize the operational characteristics to best meet the needs of the overall network. This is achieved by self-optimization routines within the overall self-organizing network, SON software.

• Self-Healing: Self-healing, as regarded as an event- driven process and aims to resolve the loss of coverage or capacity once a cell/site failure happens. Any system will develop faults from time to time. This can cause major inconvenience to users; however it is often possible for the overall network to change its characteristics to temporarily mask the effects of the fault. Boundaries of adjacent cells can be increased by increasing power levels and changing antenna elevations, etc. This self-healing aspect of SON, self- organizing networks is of great interest.

4. Requirements and Challenges.

In order to maintain the desired security level in a self-organized mobile ad hoc network a node that is responsible for its own security should carry out security monitoring or measurement of the security level. The management of security becomes easier if suitable metrics can be developed to offer evidence of the security level or performance of the network. Intrusion detection and prevention (IDS/IPS) techniques can be applied for this purpose. However, current state-of-the-art IDS/IPS techniques are not able to adapt well to dynamic situations and to address security as a multi-disciplinary issue [9]. The ultimate security objectives in opportunistic networks include: availability, authentication, confidentiality, integrity, non-repudiation and non-impersonation. The whole network system should enable its survivability whenthere are Denial of Service and Black Hole attacks in network. Each node should have the ability to ensure the identities of the nodes which it will communicate with and can check the integrity of the messages which it received. The source nodes need to ensure the confidentiality of the messages which they send, and no one could get any information from the messages except the destination nodes. Besides that, the source nodes cant deny their operations of sending or forwarding messages which they really did [10].The requirements to be met in order to develop the SON functionalities can be classified in technical and business requirements. The purpose of the technical requirements is to help in the development of novel algorithms and functionalities and to highlight the relevant network characteristics for self organization. The list of the technical requirements to be addressed comprises of performance and complexity, stability, robustness, timing, interaction among SON functionalities, architecture and scalability, and required inputs. Defining the business requirements helps to consider factors related to the involved operational costs and incorporate them while developing the solutions. The important challenges for designing effective and dependable self-organization functionalities in future mobile radio networks are issues such as determining what kind of data are required, at what rate they should be collected, and also devising techniques for collecting them. Reliability of SON methods in order to minimize human intervention, the control decisions should be reliable and operate autonomously [4].Self-organized WANETs can be informally visualized as a group of wireless communication devices, held by people without any pre-planning, coming together to form a network for a common purpose (e.g., emergency response). The problem is how to exploit those primary security associations to provide secure communication for arbitrary node pairs when needed. Neighbor authentication provides hop by hop security for secure communications in all kinds of networks. This is especially crucial for WANETs since every node need to act as the router to forward packets for others. If the node cannot authenticate its physical neighbors, how will it trust all neighbors to handle its packet correctly? Obviously, neighboring nodes with can authenticate each other directly with pre-configured keying materials. Since the number and the distribution of primary security associations are determined by the embedded social network (e.g., trust relations) of users, a node may not have primary security associations with any of its physical neighbors. In this case, a Neighbor Authentication Protocol (NAP) is required to set up derived security associations with its neighbors on the need basis with the help of already authenticated neighbors [10].

5. Routing protocols in self-organizing networks

For self-organizing networks are currently a huge number of routing protocols can be classified into three groups: reactive, proactive and hybrid. At the same time all nodes in the network must support routing protocols and carry out a choice routes, provide a guaranteed delivery of packets and high the network performance and other characteristic. Proactive routing protocols periodically send service messages over the network with information about all changes in topology. As a result each node on the base of this information builds routes to all nodes and saves them in routing table. The routes are read if necessary to send a message to any destination. Reactive protocols make up routes to specific node only when necessary to transfer information. For this the send- ing node transmits the broadcast message to network which need to reach destination node. In response the destination node transmits a confirmation message from the sender learns the desired route and saves it in routing table. For resend message the route just read from routing table. If route is not found will be to running the process of maintaining the route which is in fact searches a new route to the destination. Hybrid protocols combine the mechanisms of proactive and reactive protocols. Usually they divide the network into multiple subnets inside which operates a proactive protocol and the interaction between them is performed by reactive methods. In large networks it allows to reduce the size of routing tables which are lead to nodes in the net- work because they need to know the exact routes only for nodes subnet to which they belong. Also reduced volume of service traffic who transmitted at self-organizing network. The main part this traffic distributed only within the subnet. Routing protocols for self-organizing networks must have a short time to build routes, high reliability of packet transmission, the minimum volume of service information, prevents of the loops, find and recover routes, provide high performance and scalability [6].

6. Bio inspired techniques to network security

With the growing importance of communications techniques, more complicated communications networks are being designed and developed. The challenges of dealing with the vast complexity of networking problems (e.g., adaptive routing, congestion control, and load balancing) accentuate the need for more intelligent network layer techniques. As inspired by insects such as ants and honey bee several mobile agent-based paradigms have been designed to solve the control, routing and load balancing problems
in communications networks. Security mechanisms are critical to operating and maintaining SON systems, in which the massively distributed operations and decentralized control paradigms are essentially performed. Enormous security mechanisms have already been applied to combat malicious attack, node failure, and other kinds of threats. Among those techniques, the most well-known bio- inspired approaches is AIS.
AIS (Artificial Immune Systems Artificial): The primary goal of AIS is to efficiently detect changes in the environment or deviations from the normal system behavior in complex problems domains, and to automatically memorize these characteristics. According to the given shape-space and the affinity measure, AIS can be used efficiently for general- purpose anomaly detection. The normal behavior of a system is often characterized by a series of observations over time, and the problem of detecting novelties or anomalies can thus be viewed as finding deviations in a characteristic property in the system. AIS has also shown brilliant results for misbehavior detection and helps in designing and implementing the secu- rity framework in WSNs Furthermore, a bio-inspired secure autonomous routing mechanism called BIOSARP, which is based on ACO routing algorithm, has also been proposed for WSNs to treat the attack issues successfully. Besides wireless networks, designing scalable security mechanisms is particularly critical in transparent optical networks (TONs) due to the high speeds and transparency inherent in them. The basic idea of TONs security mechanism is: the desired global goals (e.g., the efficient failure management, detection and location, etc.) are first defined, followed by some local interactions and processes being developed to achieve those system-wide goals. A new self-organized method, as analogous to the human immunization systems primary defense mechanism, is proposed to enable the network autonomously and persistently adapt to network changes by learning newly observed vulnerabilities, while at the same time obviate the effort to exploiting already discovered ones. Furthermore, the immune-network theory can also be used to suppress or encourage multi-agent behavior and for approaches such as collaborative mine detection [3].

7. Conclusion

Wireless networks are common place nowadays and almost all modern computing devices support wireless communication in some form. These networks differ from more traditional computing systems due to the ad hoc and spontaneous nature of interactions among devices. These systems are prone to security risks, such as eavesdropping, and require different techniques as compared to traditional security mechanisms. This paper intended to give a general overview of self organizing Networks (SON), their fundamental features and challenges to wireless networks. The dynamic nature of self organizing networks in terms of node behaviors, traffic and bandwidth demands completely new approaches. Thus, communication techniques or methods that are highly dynamic must be developed for the next generation network architecture. There is a possibility that any new adversary node may join a network during self organization which will create enormous problems. Therefore, ensuring that only authentic nodes join the network at the time of self organization is also necessary. For the future work, we will continue to investigate the scheme and improve this proposed system to enhance the detection efficiency.

References

[1] D. Duan, L. Yang, Y. Cao, J. Wei, & X. Cheng, ” Self-Organizing Networks: From Bio Inspired to Social-Driven” Intelligent Systems, IEEE, vol 29, pp. 86-90, 2014.

[2] M. Behjati, J. Cosmas, & S. Member, ” Self-Organizing Interference Coordination for Future LTE-Advanced Network QoS Improvements” International Symposium

on Broadband Multimedia Systems and Broad- casting (BMSB), IEEE, pp. 1-6, 2014.

[3] Z. Zhang, K. Long., J Wang, & F. Dressler," On Swarm Intelligence Inspired Self-Organized Networking: Its Bionic Mechanisms, Designing Principles and Optimization Approaches" Communications Surveys Tutorials, IEEE, vol 16, pp. 513-537, 2014.

[4] N. Marchetti, & N.R Prasad," Self-Organizing Networks: State-of- the-Art, Challenges and Perspectives" 8th International Conference on Communications (COMM), IEEE, pp. 503508, 2010.

[5] R. A. F Erru., O. R. S Allent, & R. A Gusti," Self-Organizing Networks in 3Gpp: Standardization and Futuretrends" Communications Magazine, IEEE, vol 52, pp. 28-34, 2014.

[6] A. Proskochylo, A. Vorobyov& M. Zriakhov," Overview of Possibilities to Improve Efficiency of Self-Organizing Networks" First International Scientific-Practical Conference Problems of Infocommunications Science and Technology, IEEE, pp. 118-119, 2014.

[7] R. Savola& I. Uusitalo ,"Towards Node-Level Security Management in Self-Organizing Mobile Ad Hoc Networks" , pp. 25-32, 2006.

[8] C. Elliott, & B. Heile, "Self -Organizing , Self -Healing Wireless Net works", pp. 355-361, 2000.

[9] X. Chen, T. Youliang, L. Guangsong, M. Jianfeng " Security inopportunistic networks" International Conference on Industrial Control and Electronics Engineering (ICICEE), pp. 6-9, 2012.

[10] C. Zhang, &Y. Fang," Scalability and Security of Self-Organized Wire- less Ad Hoc.

Author Profile

JuniorikaLyngdoh, is working as an Assistant professor in Martin Luther Christian University, India. She received her master degree in computer Applications from NEHU (India) in 2010 .and currently doing Ph.D. in IT from NEHU.

Hemanta Kumar Kalita is working as Associate Professor and Head of Department of Information Technology of North Eastern Hill University, Shillong, India. He has received Ph.D. from Jadavpur University, Kolkata, India. He has six years of industry/R&D experience and around eleven years of teaching experience in both under graduate and post graduate level. His areas of research interest are Big Data Analysis, Adhoc Network Security, Performance Engineering, Spatial Data Mining, Artificial Intelligence, etc. He has one patent to his name and published several papers in International and National Journal and Conferences. He has received FOSS INDIA AWARD in 2008 awarded by LINUX FOR YOU magazine for his contribution to open source in WANem project