Randomized Replication based on Multilevel of Security for Opportunistic Network

Tawiwat Veeraklaew, Jiradett Kerdsri, and Settapong Malisuwan

***Abstract*—Networks have become a big part of the critical infrastructure of most operations. Several research funding agencies are encouraging research on revolutionary networking architectures to succeed traditional inefficient networks. The ability to rapidly create advanced technological solutions in response to user demands is key action in driving the smart networking such as active/programmable network. With the advance in current virtualization network technology, it is feasible to implement the proper network that suit the complexity of any environment. This software defined network can address the limitation of conventional network in various form. Most opportunistic networks utilize locally collected knowledge about node behavior to predict the delivery probability of each node to consider forwarding decision. To date, none of the routing protocol concerns about the sensitivity level of message in the network. This paper proposes Randomized Replication based on Multilevel of Security for opportunistic network (RRMS), a routing technique of message replication based on the randomize value of replication density. In addition, the multiple level of security is utilized as matrices of message prioritization.**

***Index Terms*—RRMS, network visualization, performance evaluation**

I. Introduction

The advent in networking technology particularly in the virtualization technique [1] eases the expediency in customizing software defined network such as OpenFlow [2]. Customization of software defined network is brought about because these advanced networking technologies allow inclusion of specific characteristics required by particular networks for instance, military tactical networks. "Virtualization provides isolation and sharing of substrate resources including routers, switches, and end-hosts which enables a flexible internet architecture that is capable of accommodating multiple architectures" [3], [4]. The idea of implementing a smart network has long been developed as a new emerging network technology "with ability to rapidly create and deploy transport, control and management architectures in response to new service" such as active/programmable network [5]. With the current networking technology, it is feasible to implement the software defined network that serve the complexity of extreme environment such as opportunistic network. The advent of intelligent mobile devices and wireless opportunistic contacts allows users to experience novel ways of sharing and retrieving content ubiquitously even under the limitation caused by link intermittency. The availability of variety of routing solutions makes it difficult to comprehend the best position solution as different routing solutions since each follows a different evaluation method [6]. Nevertheless, these network paradigms have not yet been resolved. Although multiple level of security (MLS) plays a crucial role in military communication, the lack of this function has handicapped military communication to a certain extent. Generally, multilevel security is critical to accommodate different sensitivity levels of information and different clearance levels of users [7]. Therefore, this paper seeks to propose the use of network virtualization technique to originate a new opportunistic network routing concept for military communication which accommodates different data security levels. Most opportunistic routing solutions are simulated on the basis that the movement of nodes is unpredictable and there is no information on a precise location of a node. However, messages must be forwarded considering the time and place, and are based on information such as mobility patterns, data or other essential information [8].

This paper seeks to propose an efficient and advanced routing design including related work on network virtualization, active/programmable network and opportunistic network. Discussion on concept of routing in intermittent connected mobile ad hoc network is based on the content of data. This paper will also provide the results of the researchers' simulation and illustrate the performance of proposed routing network under diverse conditions. Lastly, we seek to provide recommendations for further research in advanced routing solutions.

II. Background

A. Network Virtualization

"Network Virtualization is the process of integrating hardware and software network resources and functionality into a single, software-based administrative entity. By allowing multiple heterogeneous network architectures (service provider) to cohabit on a shared physical substrate (infrastructure provider), network virtualization provides disruptive technology which will aid in the design of various types of complex network architecture" [4]. This is an ideal infrastructure for designing the network architecture for military communications. Multiple coexisting logical networks is classified into four types which are "VLANs, VPNs, Active and Programmable Networks, and Overlay Networks" [9]

Manuscript received March 20, 2013; revised May 25, 2013.

doi: 10.12720/ijeee.1.2.115-119

Virtual Local Area Network (VLAN): “A group of network hosts sharing common set of requirements with a single broadcast domain regardless of their physical connectivity” [9]. The administration of VLANs is effortless because VLANs works on the basis of logic rather than physical connections [9]. Moreover, VLANs provide elevated levels of isolation.

Virtual Private Network (VPN): A method of computer networking to connect remote sites using private and secured tunnels over shared or public communication networks — typically the Internet. The main use of VPN is to securely connect geographically distributed sites. Basically VPN can be classified into broad categories based on layer protocol, which are layer 1, layer 2, layer 3 and higher layer VPNs.

Active/Programmable Network: A programmability pattern that added to traditional network allowing packets to dynamically modify the operation of the network making it more complex, flexible and cost-efficient. These networks are active/programmable in the sense that nodes can perform customized computations on the packets flowing through them [1]. There is two approaches emerged for this concept implementation: The Open Signal and The Active Network Approach.

Overlay Network: A computer network built on top of multiple existing physical networks. For instance, cloud computing and peer-to-peer network are overlay networks running on top of the Internet. In Fact, the Internet itself is an overlay on top of the telecommunication network.

B. *Active/Programmable Network*

Active networks are an “approach to network architecture in which the switches of the network perform customized computations on the messages flowing through them” [10]. This architecture is composed of execution environments consisting of active hardware, capable of routing and executing code within the active packets. The routers or switches in active network carry out customized computations on the packets going through them. “These active routers or switches can interoperate with legacy routers, which transparently forward datagrams in the traditional manner” [5]. Active networks permits the network nodes to conduct data computations and introduce customized programs into node of the network, which can alter, store or redirect user data going through the network. Therefore, the active network creates opportunities to support applications that traditional networks have not been able to in the past [11]. The concept of active network is similar to other approach trying to solve current networking problems such as “web proxies, multicast routers and video gateways etc that perform user driven computations in the network” [11].

There are two approaches to implement active networks:

- The Discrete Approach (Programmable Node) : This method the programs are introduced into the programmable active node (switch or router) which is separate from actual data packets that flows through the network. The program from user would send to active node to store and execute when packet arrives at the node. The data available in the packet will guide the node as to how to handle the packet.
- The Integrated Approach (Encapsulation): In this approach, the program is included in every data package that traverses through the network. When these encapsulated packets arrive at the active node, the program within the packet is interpreted and the embedded data is sent based on the instructions comprehended from the programs. Therefore every “active node has a built-in mechanism to load the encapsulated code in order to execute”.

A demand to add new service and customize existing network service has been increasing to match new application needs. The simplifying of network service development which aiming to create network that supports the service implementation and deployment process is the primary goal of programmable networking [12].

Most programmable network researches suggest that network architectures can be adapted to accommodate open programmable interface definition such as network APIs along with a range of services and toolkits. Two schools of thoughts have emerged as the implementation of programmable network: Open Signaling [13] and Active Networks [14].

- Open Signaling (OPENSIG): A series of international workshops, Open Signaling, was established in 1995 [5] to ensure Internet and Mobile Networks and Automatic Teller Machines (ATM) are more explicit, extensible, and easily programmable [13]. The OPENSIG adopts a telecommunication method that is clearly different between transport, control, and management that support programmable networks and emphasize on service creation with QOS (Quality of Service) [13]. Modeling Communication hardware which employs open programmable network interface allows explicit access and routers hence, permitting new and distinct architectures and services development. Subsequently, IEEE P1552 standard project was set up to “establish an open architecture in network control and the interface between network control and management functions” [15].
- Active Networks (AN): This school consisting of a large number of diverse AN project was established by DARPA. “Active networks promote dynamic services deployment at runtime within the confinement of existing networks”[9]. Routers or switches in AN can carry out customized computations that are based on data in active packets. Active networks “offer maximum customization of network services at packet transport granularity and offer more flexibility than the OPENSIG approach at the expense of a more complex programming model”[9].

C. Opportunistic Network

Opportunistic Networking (ON) is a new and advanced networking paradigm that utilizes contact opportunities and nodal mobility to transmit data from one node to another. In the infrastructure networks, conventional information such as network topology is used to router messages. Contrarily, ON requires new techniques ability to cope with limited or no information about evolving dynamic network topology and scenarios. In essence, ON "is recognized as an evolution of the connected MANET paradigm that mobile nodes can communicate with each other even without a complete route established between them at any time" [16], [17]. With this dynamic and unpredictable topology, context-awareness such as network formation and connectivity can aid alleviate known key matrices deriving from irrational approaches where relevant data is not used. In fact, analysisng future behavior of the users on network utilization by through past and historical information is handy to deliver messages thereby mitigating pressure and stress on network resources.

D. Opportunistic Routing

Normally ON routing scheme can be defined in two approaches: forwarding based and flooding based schemes. In forwarding based routing, there is only one single keeper for each message to forward message to its intended destination. On the other hand, flooding based approach is generation of multiple copies of the same message routing independently to increase efficiency and robustness [18].

The forwarding based scheme can be classified into three categories:

- Direct-transmission: the message generated by source node is hold at the origin until it reaches the destination node.
- Location-based: nodes transfer messages to neighbors that are closest to the end-point.
- Knowledge-based: the source and intermediate nodes decide which node to forward the messages based on certain knowledge about the network, moreover it also indicates whether the message should be transmitted immediately or put on hold until a better node can be reached.

The flooding based approach can be divided in to two types:

- Epidemic routing: this routing utilizes the epidemic algorithm by trying to send each message to all nodes in the network.
- Estimate/Prediction routing: nodes use the estimation of the likelihood of the node reaching the destination to decide it should put on hold or wait for a better option and also it gets to decide which nodes to use.

However, none of these method concerned about the data sensitivity in order to transmit the message.

E. Randomized Replication based Routing Implementation

The goal of RRMS is to concentrate on the constraints posed on military communication and also to increase the efficiency of operation. "The routing capability in military communication is crucial especially when the mobility, environmental factors, or jamming causing the disconnection" [4]. Each packet must find the best available path to reach the destination. By deploying RRMS concept, this software defined routing can be designed in virtualized software in the application layer [18] such as OpenFlow. Basically, a priori knowledge about the network topology in opportunistic networks is not mandatory. In fact, these opportunistic networks instead are routes by computing each path that should be taken while a packet is forwarded. So, each node receiving a message for a destination should exploit local knowledge to choose which the best path to be taken, among its alternatives, to eventually reach the end-point [19].

The data dissemination in RRMS develops in three simple steps [4]. First step, the data classification is initialized from user applications according to five military security levels: top secret (TS), secret (S), restrict (R), classified (C) and unclassified (U) [4]. Next step, each level carries different objectives which are significant level, security level and delivery deadline. TS or the top secret data is the most significant and should have the highest security clearance short data expiration period. Finally, priority and replication level of each data is calculated from configured objectives. Therefore, top secret data has highest priority and low replication. Higher data security prevents data replication. While insignificant data must have higher replication level to ensure it gets delivered where it is intended.

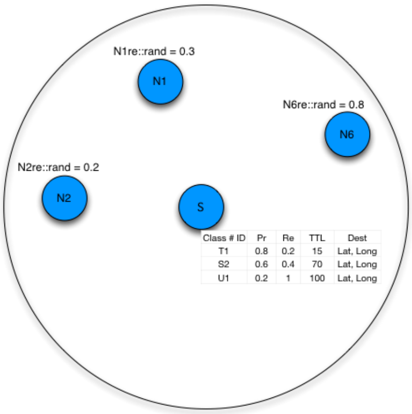
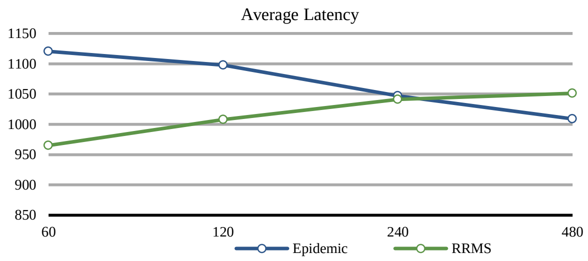


Figure 1. Replication model in RRMS

After replication level is computed, this Re value is then stored in the node table. Each message consists of Pr and Re level according to its degree of sensitivity. When the node gets contact opportunity, the node select the random number in the range of (0 – 1). Then this node can compare its message Re level to the random number. The node can transmit the message with Re level lower than the random number. Take Fig. 1 as an example, the message T1 with Re level 0.2 can transfer this message to only node N2 that contain random number of 0.2. On the other hand, message U1 can transfer to all node (N1, N2 and N6) since Re level of U1 equals to 1 which equivalent to flooding.



III. Simulation Model and Result

A. Simulation Model

Experiments were conducted to demonstrate basic characteristics of the mobility model. "Nodes were operating in 2D flat, obstacle-free environment, area was a square 1000x1000m and Communication range was set to 100m" [20]. "These simulations are carried out on the modified version of Opportunistic Network Environment (ONE) simulator" [4], [21]. The new RRMS router is implemented in the ONE simulator along with the modification of message event generator. To realize the realistic event, the sample scenario is simulated close to the actual operation. The simulation setup is based on the actual normal military tactical operation with 50 soldier nodes (one platoon). The soldier nodes are randomly moving at speed of 0.5 - 1.5 m/s. The range of transmission assumed to be 30 m. with the speed of 54 Mbps. The unique number is assigned to each node from P0 to P49. In addition, each message generated by RRMS router is tagged by its class: TS, S, R, C and U to track the messages activity. In this simulation, the numbers of messages are varied starting from 60, 120, 240 and 480 messages respectively. This routing mechanism is based on the content embedded the message. As a result, the number of messages generated from the source node can affect the performance of network. We simulated this scenario for 1 hour of operation time to study the behavior of message routing.

B. Simulation Result

The performance is evaluated by comparing three imperative aspects in opportunistic routing. "The first element is the delivery probability which is the success rate for deliveries. The second is the overhead ratio, computed as the rate of undelivered messages per completed delivery" [4]. The final element is delivery probability divided by overhead ratio which illustrates actual performance of the routing scheme. In this simulation, the RRMS is measured with commonly known epidemic routing [21]. "In epidemic routing or flood based routing, the routing mechanism employs the concept of database replication, in which a node can exchange all of the messages it has in its buffer when meeting another node" [4]. "Each node also maintains a summary vector to minimize the chance of exchanging duplicate messages" [4]. Fig. 2 shows that RRMS gain more delivery probability than Epidemic routing if the number of messages are less then 180. In Fig. 3, the overhead ratio of RRMS is significant lower than Epidemic if the numbers of generated messages are less than 200. Finally, the average delay in Fig. 4 presents lower latency of RRMS comparing to Epidemic counterpart if the number of messages are less than 240. Therefore, RRMS illustrates better performance in a limit number of messages between 60 to 200 which is approximately around 1 - 4 messages per minute.

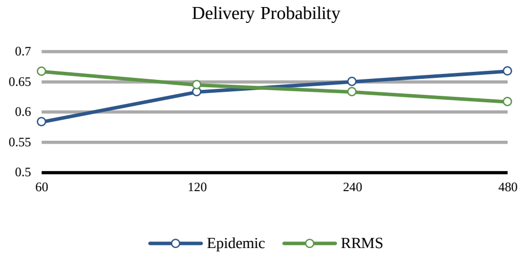


Figure 2. Delivery ratio of RRMS comparing to Epidemic routing

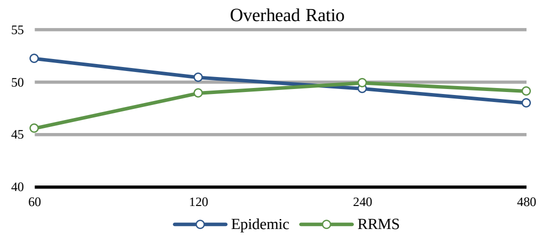


Figure 3. Overhead ratio of RRMS comparing to Epidemic routing

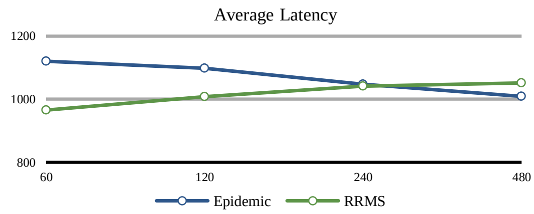


Figure 4. Average delay of RRMS comparing to Epidemic routing

IV. Conclusion

In this paper, we have presented Randomized Replication based on Multilevel of Security for Opportunistic Network (RRMS), a novel routing protocol based on the context of message without any prior knowledge of network topology. We compared the performance of RRMS with Epidemic routing by varying the number of messages generated by source node. The result shows that RRMS gain better delivery ratio, overhead ratio and average latency when the number of generated messages are less than 4 messages per minute.

References

[1] N. M. M. K., Chowdhury, and R. Boutaba, "Network virtualization: state of the art and research challenges," *Communications Magazine*, IEEE, vol. 47, no. 7, pp. 20–26, 2009.

[2] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, (2008). Openflow: enabling innovation in campus networks, openflow white paper, [Online]. Available: http://www. openflowswitch. org.

[3] S. Paul, J. Pan, and R. Jain, "Architectures for the future networks and the next generation internet: a survey," *Computer Communications*, vol. 34, no. 1, pp. 2–42, Jan. 2011.

[4] J. Kerdsri and K. Wipusitwarkun, "Data-wise routing in virtualization environment with multiple level of security for tactical network," in *Proc. 2012 IEEE/SICE International Symposium on System Integration*, pp. 933-938.

[5] A. Campbell, I. Katzela, and K. Miki, "Open signaling for ATM, internet and mobile networks (OPENSIG'98)," *ACM SIGCOMM Computer*, 1999.

[6] W. Moreira, P. Mendes, and S. Sargento, "Assessment model for opportunistic routing," in *Proc. 2011 IEEE Latin-American Conference on Communications (LATINCOM)*, pp. 1–6, 2011.

[7] J. Lee, S. H. Son, and M. Singhal, "Design of an architecture for multiple security levels in wireless sensor networks," presented at 2010 Seventh International Conference on the Networked Sensing Systems, pp. 107–114.

[8] I. Joe and S. B. Kim, "A message priority routing protocol for delay tolerant networks in disaster areas," *Future Generation Information Technology*, pp. 727–737, 2010.

[9] N. Chowdhury, "A survey of network virtualization," *Computer Networks*, vol. 54, no. 5, pp. 862–876, Apr. 2010.

[10] D. Tennenhouse and J. Smith, "A survey of active network research," *Communications Magazine*, IEEE, vol. 35, pp. 80–86, 1997.

[11] S. Munir, "Active Networks - A Survey," cs.wustl.edu. [Online]. Available: http://www.cs.wustl.edu/~jain/cis788-97/ftp/active_nets.pdf.

[12] A. M. Al-Sharafi, M. Othman, S. Subramaniam, and N. Sulaiman, "Investigating multicast tree with multiple sources in AMTree protocol," in *IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 2007*, 2007, pp. 729-732.

[13] A. T. Campbell, H. G. De Meer, M. E. Kounavis, K. Miki, J. B. Vicente, and D. Villela, "A survey of programmable networks," SIGCOMM Computer Communications, vol. 29, no. 2, Apr. 1456.

[14] comet.columbia.edu. [Online]. Available: http://comet.columbia.edu.

[15] DARPA active networks, nms.lcs.mit.edu. [Online]. Available: http://nms.lcs.mit.edu/darpa-activenet/.

[16] A. Bujari, C. E. Palazzi, and D. Bonaldo, "Performance evaluation of a file sharing DTN protocol with realistic mobility," *Wireless Days*, 2011 IFIP, pp. 1–6, 2011.

[17] J. Biswas, A. A. Lazar, J. F. Huard, K. Lim, S. Mahjoub, L. F. Pau, M. Suzuki, S. Torstensson, W. Wang, and S. Weinstein, "The IEEE P1520 standards initiative for programmable network interfaces," *Communications Magazine*, IEEE, vol. 36, no. 10, pp. 64–70, 1998.

[18] C. M. Huang, K. C. Lan, and C. Z. Tsai, "22nd International Conference on Advanced Information Networking and Applications - Workshops (aina workshops 2008)," presented at the 22nd International Conference on Advanced Information Networking and Applications - Workshops (aina workshops 2008), pp. 1672–1677.

[19] J. Kerdsri and K. Wipusitwarkun, "Network virtualization for military application: Review and initial development of conceptual design," in *Proc. 2012 14th International Conference on Advanced Communication Technology*, pp. 61–66, 2012.

[20] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks," *Communications Magazine*, IEEE, vol. 44, no. 11, pp. 134–141, 2006.

[21] M. Rollo and A. Komenda, "Mobility model for tactical networks," *Holonic and Multi-Agent Systems for Manufacturing*, pp. 254–265, 2009.

Tawiwat Veeraklaew achieved his Ph.D. in Mechanical Engineering from University of Delaware, USA. He also received his MS in Mechanical Engineering from Ohio University, USA and completed BS in Mechanical Engineering from Chulachomklao Royal Military Academy, Thailand. Currently he holds a position as a senior researcher in Defense Technology Institute, Bangkok, Thailand.

Jiradett Kerdsri graduated from University of Melbourne, Australia majoring in M.S. Geographical Information Technology. He achieved his Bachelor of Engineering in Civil Engineering from Airforce Academy, Bangkok, Thailand

From 2006 to 2008, he was a Programming Officer in Military Information Department at the Royal Thai Supreme Command Head Quarters. Currently he holds as a researcher in Defence Technology Institute (DTI). His research interests are in spatial web mapping and spatial geo-sensor network. He also specializes in 3D spatial visualization and other geographic information technology research.

Settapong Malisuwan was born on 24th March 1966 in Bangkok, Thailand. He received his PhD in electrical engineering (telecommunications), specializing in mobile communication systems from Florida Atlantic University (State University System of Florida), Boca Raton in 2000. He received an MSc in electrical engineering in mobile communications system, from George Washington University in 1996, an MSc in electrical engineering in telecommunication engineering from Georgia Institute of Technology in 1992 and a BSc in electrical engineering from the Chulachomklao Royal Military Academy, Nakhon-Nayok, Thailand in 1990. He served in the Royal Thai Armed Forces for more than 25 years and is currently the Vice Chairman of National Broadcasting and Telecommunications, Bangkok, Thailand. His research interests are in efficient spectrum management and Telecommunications policy and management in Thailand. Col. Dr. Settapong Malisuwan is currently the Elected Vice Chairman and Board Member in the National Broadcasting and Telecommunications Commission, Thailand.