A Survey of Security Issues and Routing Protocols in Mobile Adhoc Networks

Tholkapia Arasu, Ph.D.
Principal
Avs College Of Engineering
Salem

Y.Arockia Jesuraj
Assistant Professor
Sethu Institute Of Technology
Madurai

R.Kowsalya
ME(CSE),2nd year
Sethu Institute Of Technology
Madurai

ABSTRACT
Mobile Ad hoc network consist of a lot of ad hoc nodes connecting to enjoy communication. The nodes have internal capabilities and connect to the end users. There is a need for optimal path to be allocated to users. This allows for easy access and provides data in a efficient manner. The conventional algorithms in usage though efficient suffer from issues like congestion, data loss. This needs to be handled as part of the network model. There is overhead in providing data as it needs to be secured. This paper analyzes and provides directions for combining security and routing protocols in ad hoc network. A complete tabulation has been prepared and provides research directions for providing optimal and secured communication in mobile ad hoc network.

Keywords
ComputationalComplexity,PNR,SRT,,FACES,NRPA, searching algorithm.

1. INTRODUCTION
Cryptology is the art and science of information obfuscation. One of the most the paper known aspects of cryptology - that of encryption, which this thesis addresses, is found on very simple ideas. Replace each letter in a given English paragraph with the letter three positions subsequent in the alphabet, and you are encrypting with the Caesar cipher, designed millennia ago to protect the Roman general's battle orders. The paragraph encrypted is called the plaintext and the result of which is the cipher text. Identifying the plaintext without the knowledge of the key is cryptanalysis. For the simple algorithm given above, the key has only the papernty-six potential values, so the amount of secrecy employed by the algorithm is trivially small.

In addition to encryption, cryptography incorporates other related techniques, including protection and verification of message integrity, authentication and non- repudiation. It can be partitioned into two fields (symmetric and asymmetric), which relates to how cryptographic keys are used. In asymmetric cryptography, two keys are used one is visible to the initiator of the cryptographic process, and is useful for signing and encrypting documents, the other key is publicly available and useful for verifying the author of signatures and decrypting associated documents. Symmetric ciphers use a single key for the dual purpose of encryption and decryption, and for integrity protection, but are generally not used for signature generation or verification. Symmetric ciphers fall into two categories: block ciphers and stream ciphers. Stream ciphers maintain state and produce key stream which externally combined with the plaintext to make the cipher text. Stream ciphers are fast in hardware and slow in software.

Although algebraic attacks are only successful against bit-based stream ciphers, their nature pose a danger to all stream ciphers, since each bit of output generates new equation that can be algebraically solved to identify key bits. The classical example of a stream cipher is the one-time pad in which key stream bits are generated randomly and independently. Each key stream bit ki is combined with a corresponding plaintext bit pi to form the cipher text $c_i = p_i \oplus k_i$ for $0 \leq$ i< m where m is the message length. Non-random generation of the key stream bits (the pad), or duplication of portions of the pad lead to recovery of the plaintext, more easily if it possesses a high level of redundancy. When used correctly, the one-time pad is unconditionally secure. The paperyer it suffers from the requirement that the key stream needs to be as long as the message it encrypts.

2. RELATED WORK

Qayyum, Mohammed suggested a mechanism for handling data aggregation in networks. A broad variety of security threats is being presented. This approach has limitation as it does not consider the real time traffic of the network. Sheikh, R. Suggested a architecture for handling security issues in Mobile Ad hoc Network. A architecture can be proposed as part of the standard for the Mobile Ad hoc Network.

Liu Chunli suggested the different security measures that are part of the network. The different category of threats has been clearly defined and presented as part of the work. Ahmed, S analyzed the security issues of networks. The different parameters that are as part of the universities for standardizing the communication are presented.

Sen Xu/2006 performed a detailed survey of different issues that are available as part of the network. The paper identified a set of standards that can be used as part of the 802.1e standard.

Intermittently connected mobile networks (ICMN) are mobile wireless networks where most of the time there does not exist a complete path from a source to a destination, or such a path is highly unstable and may change or break while being

discovered. There are many real networks that follow this model. Examples include wildlife tracking and habitat monitoring sensor networks [1], military networks [2], vehicular ad hoc networks (VANETs) [3], pocket switched networks (PON) [4], networks for low-cost Internet provision to remote communities [5], etc. In these networks, intermittent connectivity might arise due to sparseness [5], [6], nodes path papering down to conserve energy [1], high mobility [3], or even for covertness [2]. Intermittently connected mobile networks belong to the general category of Delay Tolerant Networks (DTN) [7], that is, networks where incurred delays can be very large and unpredictable.

Conventional Internet routing protocols (e.g., RIP, OSPF) as the paper ad hoc network routing schemes, such as DSR, AODV, etc. [8], assume that a complete path exists between a source and a destination, and try to discover minimum cost paths before any useful data is sent. Since no such end-to-end paths exist most of the time in ICMNs, such protocols would fail in this context. However, this does not mean that packets can never be delivered under intermittent connectivity. Over time, different links come up and down due to node mobility (or other reasons). If the sequences of connectivity graphs over a time interval are overlapped, then an end-to-end path might exist. These implies that a message could be sent over an existing link, get buffered at the next hop until the next link in the path comes up, and so on and so forth, until it reaches its destination.

This imposes a new model for routing. Routing here consists of a sequence of independent, local forwarding decisions, based on current connectivity information and predictions of future connectivity information. Furthermore, node mobility often needs to be exploited in order to deliver a message to its destination, which is why this model is usually referred to as "mobility-assisted routing" (other names include "encounter-based forwarding" and "store-carry-and-forward"). The idea is reminiscent of the work in [9]. Hothe paperver, mobility there is exploited in order to improve capacity, while here it is used to overcome the lack of end-to-end connectivity.

Depending on the number of copies of a single message that may coexist in the network, one can define two major categories of mobility-assisted routing schemes. In single-copy schemes, there's only one node in the network that carries a copy of the message at any given time. The paper call this node the "custodian" of the message. When the current custodian forwards the copy to an appropriate next hop, this becomes the message's new custodian, and so on and so forth until the message reaches its destination.

On the other hand, multiple-copy (or multi-copy) routing schemes may generate multiple copies of the same message, which can be routed independently for increased robustness. The majority of routing schemes proposed for ICMNs are flooding-based, and, therefore, multi-copy in nature [1], [10], [11]. Despite their increased robustness and low delay, flooding-based protocols consume a high amount of energy, bandwidth, and memory space (all scarce resources for most low-cost wireless devices) [1], [10], [12]. Further, under high traffic loads they suffer from severe contention and message drops that can significantly degrade their performance and scalability [12], [13]. These shortcomings often make such algorithms inappropriate for energy-constrained and bandwidth constrained applications, which is commonly the case in wireless networks. Consequently, it is desirable to design efficient single-copy routing schemes for many resource-constrained ICMNs. Additionally, single-copy schemes constitute the building blocks of multi-copy schemes.

2.1 Multi Copy Scheme

In many multi-copy schemes a number of copies are generated, each of which is routed independently using a single-copy algorithm [12]. For this reason, it is important to have a good understanding of the tradeoffs involved in single-copy routing, in order to design efficient multi-copy schemes. With this in mind, the paper performs a thorough investigation of single-copy routing for intermittently connected mobile networks. (In [14] the paper studies the same problem using multi copy approaches.)The paper present a number of increasingly "smart" schemes, exposing their individual advantages and shortcomings, and demonstrate that competitive performance can often be achieved without the overhead and logistics of using redundant copies. The champion algorithm of our study turns out to be one that combines the simplicity of a simple random policy, which is efficient in finding good leads towards the destination, with the sophistication of utility-based policies that efficiently follow good leads. Finally, the paper proposes an analytical framework to evaluate the performance of any routing scheme in the context of ICMN. Using this framework the paper derive the lower and upper bounds on the expected delay of any single-copy routing scheme (these are actually bounds for multi-copy schemes, as the paper[ll]).The paper also use our framework to analyze the expected delivery delay of all the single-copy algorithms presented.

Although a large number of routing protocols for wireless ad hoc networks have been proposed [8], [15], traditional routing protocols are not appropriate for networks that are sparse and disconnected. The performance of such protocols would be poor even if the network was only "slightly" disconnected. To see this, note that the expected throughput of reactive protocols is connected with the average path duration PD and the time to repair a broken path t_{repair} with the following relationship:

$$throughtput = \min\{0, DateRate(1-(t_{repair} / PD))\}$$

Node mobility leads to frequent disconnections, reducing the average path duration significantly. Consequently, in most cases t_{repair} (at least 2 the optimal delay) is expected to be larger than the path duration, which implies that the expected throughput will be close to zero. Proactive protocols, on the other hand, would declare lack of a path, or result into a deluge of topology updates. One approach to deal with very sparse networks or connectivity "disruptions" [2] is to reinforce connectivity on demand, by bringing for example additional communication resources into the network when necessary (e.g., satellites, UAVs, etc.). Similarly, one could force a number of specialized nodes (e.g., robots) to follow a given trajectory between the disconnected parts of the network in order to bridge the gap [17], [18]. In yet other cases, connectivity might be predictable, even though it is intermittent (e.g., Inter-planetary networks, IPN [19]).

Traditional routing algorithms could then be adapted to compute shortest delivery time paths by taking into account future connectivity [5], [20]. Nevertheless, such approaches are orthogonal to our work; our aim is to study what can be done when connectivity is neither enforced nor predictable,

but rather opportunistic and subject to the statistics of the mobility model followed by nodes. Despite a significant amount of work and consensus existing on the general DTN architecture [7], there has not been a similar focus and agreement on DTN routing algorithms, especially when it comes to networks with opportunistic connectivity.

The simplest possible approach is to let the source or a moving relay node (Data Mule) carries the message all the way to the destination (Direct Transmission) [6]. Although this scheme performs only one transmission, it is extremely slow [9]. A faster way to perform routing in ICMNs, called Epidemic Routing, is to flood the message throughout the network [11]. This scheme is guaranteed to find the shortest path when no contention exists for shared resources like wireless bandwidth and buffer space. Yet, it is extremely wasteful of such resources. What is worse, in realistic scenarios where bandwidth, memory space, or energy resources might be scarce, the performance of flooding degrades significantly [10], [12], [13]. A number of approaches have been taken to reduce the overhead and improve the performance of epidemic routing [1], [10], [13]. In [21] the authors examine a number of different schemes to suppress redundant transmissions and clean up valuable buffer space after a message has been delivered with epidemic routing. In [13] a message is forwarded to another node with some probability smaller than one (i.e., data is "gossiped" instead of flooded).

Finally, in [1] a simple method to take advantage of the history of past encounters is implemented in order to make the and more "informed" forwarding decisions. The concept of history-based or utility-based routing is further elaborated in [10]. Results from these studies indicate that using the age of last encounter with a node, when making a forwarding decision, results in superior performance than flooding. The concept of history-based routing has also been studied in the context of regular, connected wireless networks in finally; it has also been proposed that Network Coding ideas could be useful to reduce the number of bytes transmitted. Although all these schemes, if carefully tuned, can improve to an extent the performance of epidemic routing, they are still flooding-based in nature, and thus often exhibit the same shortcomings as flooding [14].

2.2 The 2-Hop Scheme

A different approach to significantly reduce the overhead of epidemic routing, while still maintaining good performance, is to distribute only a bounded number of copies [12]. In a manner similar to the 2-hop scheme of [9], a copy is handed over to a fixed number of relays, each of which can then deliver it only directly to the destination. Nevertheless, in many situations where node movement is strongly correlated or predominantly local, the performance of this scheme deteriorates [4], [14]. Despite the variety of existing approaches, the majority of them are multi-copy ones. Furthermore, the minority that deals with single-copy techniques only studies direct transmission [6] or some form of utility-based schemes in relatively different contexts.

In this work, the paper perform a detailed inquiry into the problem space of single-copy routing, and show how to achieve competitive performance without using multiple copies. The paper look into how utility functions can be designed to fully take advantage of the "field" of past encounters, and propose a function that is shown to achieve up to an order of magnitude improvement in ICMNs over existing utility functions. Finally, the paper propose a novel, hybrid routing scheme, which uses randomization when necessary to overcome some inherent shortcomings of utility-based forwarding.

In the theory area, a large body of work has recently emerged trying to analyze the trade-offs involved between the asymptotic capacity and the asymptotic delay of the 2-hop scheme proposed in [9], and related schemes exploiting mobility. Although asymptotic results provide valuable insight on the scalability of a given family of protocols, they often do not provide the necessary insight to design efficient and practical schemes. Furthermore, the majority of these works are concerned with delay in connected networks. In such networks, mobility is only used to reduce the number of transmissions. On the other hand, mobility in disconnected networks is an intrinsic component of the minimum delay. Furthermore, in connected networks the transmission range of each node has to scale with the number of nodes, in order to ensure connectivity, making all related analytical results strictly a function of the number of nodes.

Here, the interested in a much wider range of connectivity scenarios, where transmission range, number of nodes, and network size are independent parameters, whose individual effect on performance our analytical framework aims at quantifying. Also, in the context of disconnected networks, most existing analytical efforts concern the performance of epidemic routing or other multi-copy schemes To the best of our knowledge, the only prior analytical work for single copy schemes is on direct transmission [6] and some asymptotic results regarding utility-based schemes. Finally, in many existing studies, some parameters of the proposed model (e.g., node inter-meeting times) need to be acquired from simulation traces for each and every scenario [21]. Here, the paper expand our framework from to evaluate the delivery delay of all the single-copy algorithms examined, as the paper[ll] as to derive lower and upper bounds on the expected delay achievable by any scheme in ICMNs.

2.3 Single-Copy Routing Strategies

In this section, the paper explores the problem space of sing le-copy routing in ICMNs. Our problem setup consists of a number of nodes moving independently according to some stochastic mobility model. Additionally, the paper assumes that the network is disconnected at most times, and that transmissions are faster than the node movement (a reasonable assumption with modern wireless devices1). Also, each node can maintain a timer for every other node in the network, which records the time elapsed since the two nodes last encountered each other (i.e., came within transmission range). These timers are similar to the age of last encounter in [25], and are useful, because they contain indirect (relative) location information. However the paper, note that not every routing scheme requires these timers. Also, the paper assumes that this is the only information available to a node regarding the network (i.e., no explicit location info, etc.). Finally, the paper assumes that nodes emit a beacon signal, possibly periodically, that advertises their presence.

In practice, when another node senses this beacon, the two nodes establish a relationship (as for example in Bluetooth pairing [33]) by exchanging IDs and other relevant information like timer values. The paper refers to this as an "encounter".2 the paper will now look into a number of

increasingly "smart" routing strategies. The paper believes that these are fairly representative of different approaches one might take for the problem in hand.

Each routing algorithm decides under what circumstances a node, currently holding the single message copy, will hand it over to another node it encounters. The goal is that each forwarding step should, on the average, result in progress of the message towards its destination. (Due to space limitations, all the proofs for this section can be found in direct Transmission: The simplest possible routing scheme imaginable is the following: a node a node A forwards a message to another node B it encounters, only if B is the message's destination.

This scheme is trivial, but it has the advantage of performing only a single transmission per message. It has been considered in some previous work [6], [9], and its expected delivery delay is an upper bound on the expected delay of any routing scheme. It will therefore serve as our baseline. Randomized Routing Algorithm: The first nontrivial routing algorithm that the paper will look at is a randomized forwarding algorithm, where the current message custodian hands over the message to another node it encounters with probability $p \in (0,1].$

Further, in order to avoid a message constantly jumping back and forth between the two nodes within range, the paper assume that, when a node receives a message, it is not allowed to send the message back to the node it received it from, for a given amount of time (the two nodes are tagged as "coupled" [35] until a timer expires).For many non contrived (or non adversarial) mobility models, it can be shown that a smaller timer value on average implies a smaller distance from the node in question. Therefore, the paper can define a utility function based on these timers, which indicates how "useful" a node might be in delivering a message to another node. A gradient-based scheme can then be used to deliver a message to its destination, as has been noted in [10].This scheme will try to maximize the utility function for this destination.

The above lemma, as in the case of Randomized Routing, holds for a number of mobility models like Random Walk, Random Waypoint, Community-based mobility etc. Utility-Based Routing with Transitivity: Despite making better forwarding decisions than randomized ones, the previous scheme suffers from a "slow start" phase, which is more manifested in large networks. In a large network, where source and destination are usually far, almost all nodes around the source will have moved long enough to get "decoupled" from the destination.

Thus, they will not have a high enough utility to become next hops. Additionally, if it happens that the few nodes around the message custodian last met the destination before the custodian did, the custodian will probably have to wait a long time until it moves close to the destination again (even if a connected path to the destination existed). The reason for this inefficiency is that each node updates its utility function for the destination only when it encounters that destination. Location information takes a very long time this way to get diffused throughout the network, and by the time such information does get diffused it has become obsolete.

2.4 Seek and Focus Routing

A Hybrid Approach: Although the use of transitivity does alleviate the slow start phase, if nodes move fast enough, even transitivity might not be able to diffuse utility information promptly throughout the network. Additionally, utility values of nodes can be seen as a time-varying utility field with the global maximum at the destination. Since a greedy forwarding approach is used, the message often gets stuck at local maxima for some time. In order to deal with these shortcomings, the paper propose a hybrid routing protocol, called "Seek and Focus", which aims to combine the best of both worlds. It can escape the slow-start phase and local maxima of utility-based protocols, while still taking advantage of the higher efficiency of utility-based forwarding.

Initially it looks around greedily for a good lead towards the destination using randomized routing, and then uses a utility-based approach to follow that lead efficiently. Additionally, it uses a procedure reminiscent of the "peripheral routing" in some position based routing protocols to prevent a message from getting stuck for a long time at local maxima of utility.

2.5 Oracle Based Routing

An "Oracle-Based" Optimal Algorithm: The algorithm that minimizes the expected delivery delay is aware of all future movement, and, thus, it is an "oracle-based" algorithm. Based on this knowledge, it computes the optimal set of forwarding decisions (i.e., time and next hop), which delivers a message to its destination in the minimum amount of time.

The "oracle-based" algorithm cannot be implemented in reality, when connectivity is opportunistic. It provides an offline solution to an inherently online problem, and, thus, its delay will serve as a lower bound on the delay of any routing strategy. (Note that, when future connectivity is known, it could be possible to implement this scheme, albeit with considerable overhead [5].) Finally, notice that, under the assumption of infinite buffer space and bandwidth, flooding (i.e., epidemic routing) achieves this minimum delay.

3. CONCLUSION

This paper explores the different approaches that are available for handling security threats in networks. A complete analysis has been presented for handling the different problems in networks. The outcomes of the survey is given below:

- The network can be improved with more level of computations as part of the standards.
- The network can be optimized by combining with optimization algorithms. It can be approaches like Ant colony optimization.
- The learning part of the network can be improved by using neural network and fuzzy approaches.

4. REFERENCES

[1] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Single-copy routing in intermittently connected mobile networks," in Proc. IEEE Conf. Sensor and Ad Hoc Communications and Networks (SECON), 2004, pp. 235–244.

[2] P. Gupta and P. Kumar, "Capacity of wireless networks," IEEE Trans. Inf. Theory, vol. 46, no. 2, pp. 388–404, 2000.

[3] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter, "Mddv: Mobilitycentric data dissemination algorithm for vehicular networks," in Proc. ACM SIGCOMM Workshop on Vehicular Ad Hoc Networks (VANET), 2004.

[4] R. C. Shah, S. Roy, S. Jain, and W. Brunette, "Data mules: Modeling and analysis of a three-tier architecture for sparse sensor networks," Elsevier Ad Hoc Netw. J., 2003.

[5] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott, and H.The paperiss, "Delay-tolerant networking: An approach to interplanetary Internet," IEEE Commun. Mag., vol. 41, no. 6, pp. 128–136, Jun. 2003.

[6] J. Heidemann, W. Ye, J. Wills, A. Syed, and Y. Li, "Research challenges and applications for underwater sensor networking," in Proc. IEEE Wireless Communications and Networking Conf., 2006.

[7] J. Scott, P. Hui, J. Crowcroft, and C. Diot, "Haggle: A networking architecture designed around mobile users," in Proc. IFIP Conf.Wireless On-Demand Network Systems and Services (WONS), 2006.

[8] M. Papadopouli and H. Schulzrinne, "Seven degrees of separation in mobile ad hoc networks," in Proc. IEEE GLOBECOM, 2000.

[9] C. E. Perkins, Ad Hoc Networking, 1st ed. Reading, MA: Addison- The papersley, 2001.

[10] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Duke Univ., Durham, NC, Tech. Rep. CS-200006, Apr. 2000.

[11] P. Juang, H. Oki, Y.Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with Zebranet," in Proc. ACM ASPLOS, 2002.

[12] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," SIGMOBILE Mobile Comput. Commun. Rev., vol. 7, no. 3, 2003.

[13] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," in Proc. IFIP Networking, 2006.

[14] Q. Li and D. Rus, "Communication in disconnected ad hoc networks using message relay," J. Parallel Distrib. Comput., vol. 63, no. 1, pp. 75–86, 2003.

[15] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott, and H.The paperiss, "Delay-tolerant networking: An approach to interplanetary Internet, IEEE Commun. Mag., vol. 41, no. 6, pp. 128–136, Jun. 2003.

[16] Qayyum, Mohammed; Subhash, P.; Husamuddin, Mohammed, "Security issues of data query processing and location monitoring in MANETS", International Conference on Communication, Networking & Broadcasting,pp.1-5,2012

[17] Sheikh, R.; Singh Chande, M.; Kumar Mishra, D.," Security issues in MANET: A review", Seventh International Conference On Wireless And Optical Communications Networks (WOCN), pp.1-4,2010

[18] Liu Chunli; Liu DongHui ," Computer network security issues and countermeasures", IEEE Symposium on Robotics and Applications (ISRA), Pp.328-331,2012

[19] Ahmed, S.; Buragga, K.; Ramani, A.K. ,"Security issues concern for E-Learning by Saudi universities", 13th International Conference on Advanced Communication Technology (ICACT), Pp.1579-1581, 2011