IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 2, No. 1
February 2013

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

Int. J. Engg. Res. & Sci. & Tech. 2013

IJERST International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 2, No. 1, February 2013

Research Paper

IMPACT OF ZERO KNOWLEDGE PROTOCOL ON DELAY TOLERANT NETWORK ROUTING

P Maitreyi[1*] and M Sreenivasa Rao[2]

Corresponding Author:* ***P Maitreyi,* ✉ *maithri_p@yahoo.co.in*

Delay Tolerant Networks (DTNs) are wireless networks in which at any given time instance, the probability of having a complete path from a source to destination is low due to the intermittent connectivity between nodes. Several routing schemes have been proposed for such networks to make the delivery of messages possible despite the intermittent connections. In this paper, in addition to intermittent connectivity which impacts routing most strongly, we also analyze the effects of underlying zero knowledge protocol proofing system over the communication network. In this network, nodes interact in diverse ways so that some nodes meet each other more frequently than others. In the paper, we first propose a new network model to reflect the underlying zero knowledge protocol proofing system over the network nodes, then we study the effects of this model on the performance of multi-copy based routing algorithms.

Keywords: Delay and Disruption Tolerant Networks, MANETs, ZKP, key exchange, Peggy, Victor

INTRODUCTION

.Delay Tolerant Networks (DTN) are wireless networks in which nodes are intermittently connected and there is no guarantee that a path exists from source to destination at any time instance. Today, there are many examples of such networks including wildlife tracking networks (Juang *et al.*, 2002), military networks (http://www.darpa.mil/ato/solicit/DTN/) and vehicular networks (Ott and Kutscher, 2005). Moreover, the rapid and wide spread of different kinds of devices with wireless capabilities among people and their surroundings has enabled the possibility of opportunistic urban routing of messages in social networks. Such mode of communication, especially if combined with sensing (monitoring traffic, etc.), attracted a great deal of interest because of enormous potential of collaborative data gathering via already deployed and human maintained devices, including cell phones and GPS devices.

Since the standard routing algorithms assume that the network is connected most of the time, they can not be applied to the routing of messages

[1] Department of IT, MGIT, Hyderabad, India.

[2] School of IT, JNTUH, Hyderabad, India.

in a delay tolerant network. There are many routing algorithms proposed for such networks. Since the connectivity of the nodes is intermittent, these algorithms make use of *store-carry-and-forward* paradigm in which messages are stored at nodes until an opportunity (meeting a new node) arise to forward the message. Although these proposed algorithms base their designs on different assumptions, the most appropriate assumption for real delay tolerant networks is zero knowledge about the network. In other words, since the future node contact times and their durations often can not be known exactly in a real DTN, the routing algorithms making their decisions based only on their local observations are the most useful ones.

Although many routing algorithms for DTNs were proposed in the literature, very few of them take into account the effect of zero knowledge protocol proofing system on the design of the routing algorithm. The movement of nodes in a mobile network and the interactions between nodes is not purely random and homogeneous but it is somewhat a mixture of homogeneous and heterogeneous behaviors. In other words, in a real mobile network, we always see grouping of nodes into communities such that the nodes within the same community behave similarly and the nodes from different communities show different behaviors.

Consider a Pocket Switched Network (PSN) which is a kind of mobile network in which people are intermittently connected via different wireless devices including cell phones and GPS devices. The connectivity between these human carried devices is achieved when they get into the range of each other. In a social network, the relationship defining the frequency of connectivity between nodes can be various interdependencies including friendship, trade and status. That's why, for an efficient routing of messages in such networks, the mobility of nodes and the underlying community structure of the members of the whole society has to be carefully analyzed. For example, consider a high school network. Students in the same class have higher chance to see (so also to transfer data to) each other than the students from other classes (i.e. they can probably meet only during breaks).

In this paper, we studied the effect of the zero knowledge protocol proofing system in a delay tolerant network and show that considering this structure can help designing better routing algorithms with security. Since most of the routing algorithms for DTNs utilize the idea of distributing multiple copies of the same message, in this paper we study the effects of zero knowledge protocol proofing system of the network on multi-copy based routing algorithms. In the design of such algorithms for DTNs, there are two important issues to consider (Bulut *et al.*, 2008): (i) the number of copies of each message that will be distributed to the network, and (ii) the selection of nodes to which the message is replicated. Both of these issues are studied by different authors in terms of the general routing idea in delay tolerant networks (i.e., Spyropoulos *et al.*, 2008) but they are still open to research for (community-based) networks such as PSNs which change the nature of standard delay tolerant networks due to the heterogeneous inter-meeting times of nodes in the network. In this paper, we study these issues from a community based network's point of view and demonstrate how they change in this setting.

RELATED WORK

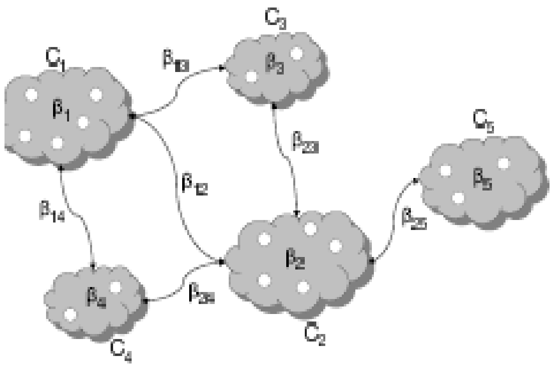
Recently, several routing algorithms have been proposed for delay tolerant networks. However, some of them have unrealistic assumptions (the existence of oracles which give information about future node meetings) which are not satisfied in real DTNs. Other than these algorithms, there are also some algorithms (Vahdat and Becker, 2000; Lindgren *et al*., 2003; Harras *et al*., 2005; Spyropoulos *et al*., 2005; Burgess *et al*., 2006; Spyropoulos *et al*., 2008; Bulut *et al*., 2008) which assume zero knowledge about the future network features (node meetings, contact durations etc.). In these algorithms, to increase the delivery rate of messages to the destination, two different approaches are applied. In the first one (i.e., Spyropoulos *et al*., 2008), multiple copies of the message are generated and distributed to the other nodes in the network and the delivery of at least one of these copies is expected in the future. Obviously, the more copies are used, the higher delivery ratio is achieved. But, on the other hand, with the increasing number of copies, network resources such as bandwidth and buffer space are wasted. In the second approach (i.e., Lindgren *et al*., 2003), a single copy of the message is transferred only to nodes having higher delivery likelihood. The histories of node meetings are utilized and possible future meetings of the nodes are predicted so that optimum paths to the destination are followed to increase the delivery ratio.

Although there are many algorithms utilizing the controlled flooding approach, only a few of them focus on message routing in social networks which also consist of intermittently connected nodes. What differentiates such networks from the general delay tolerant networks is their inner heterogeneous connectivity. In other words, there may be some set of nodes which meet more often than the others. Considering this partitioning of nodes into communities in mobile networks, there are some algorithms proposed to make the routing of messages more efficient in such networks. In, Daly *et al*. (2007, use both the between's and the similarity metric to increase the utility function containing these two metrics is calculated for each destination, then the node having higher utility value for a destination is given the messages. In each node is assumed to have two rankings: global and local. While the former denotes the popularity (i.e. connectivity) of the node in the entire society, the latter denotes its popularity within its own community. Messages are forwarded to nodes having higher global rankings until a node in the destination's community is found. Then, the messages are forwarded to nodes having higher local ranking. Thus, the probability of finding the destination's community is increased. Then, after the message reaches the destination's community, the probability of meeting the destination is increased, so that the shortest delivery delay is attempted.

NETWORK MODEL AND ASSUMPTIONS

To illustrate the general picture of communities in a DTN network, we use the following model. Assume that there are *m* communities (C1 to Cm) in the whole network and there are Ni nodes in community Ci. Moreover, assume that the nodes in community Ci get contact with the nodes in community Cj with an average intermeeting time of β_{ij} (for simplicity $\beta_i = \beta_{ii}$). In other words, they have a chance to exchange their data in every t time units where t is a random variable exponentially distributed with mean β_{ij}. The nodes within the same community are considered identical in terms of meeting behavior with other nodes, but the nodes from different communities are considered having different behaviors. Accordingly, both the homogeneity and the

Figure 1: A Sample DTN Network With Five Communities, Each Community Has Different Inner and Inter-community Meeting Rates



heterogeneity are embedded into the network structure. A sample network with five communities was shown in Figure 1.

The beauty of this model is that it successfully monitors the general behavior of nodes in community-based DTN networks. It avoids dealing with individual behaviors of nodes and provides only the average intermeeting time of nodes both inside and outside the community. Consider the examples of real life PSN scenarios. Nodes get in contact with each other depending on their relations in the society. Moreover, this contact times may sometimes happen unpredictably. However, even in such cases, we claim that on the average there are stable intra- and inter-community intermeeting times in the whole network and these can be found using the histories of node meetings.

ANALYSIS

Zero-knowledge protocols allow identification, key exchange and other basic cryptographic operations to be implemented without leaking any secret information during the conversation and with smaller computational requirements than using comparable public key protocols. Thus Zero-knowledge protocols (David Chaum, xxxx) seem very attractive especially in smart card and embedded applications. There is quite a lot written about zero-knowledge protocols in theory, but not so much practical down-to-earth material is available even though zero-knowledge techniques have been used in many applications. Some of the practical aspects of zero-knowledge protocols and related issues were discussed, in the mind-set of minimalistic practical environments. The hardware technology used in these environments was described, and resulting real-world practical problems were related to zero-knowledge protocols. A very lightweight zero knowledge protocol was outlined and its possible uses and cryptographic strengths and weaknesses were analyzed.

The parties in a Zero-knowledge protocol

The following *people* appear in zero-knowledge protocols:

Peggy the Prover

Peggy has some information that she wants to prove to Victor, but she doesn't want to tell the secret itself to Victor.

Victor the Verifier

Victor asks Peggy a series of questions, trying to find out if Peggy really knows the secret or not. Victor does not learn anything of the secret itself, even if he would cheat or not adhere to the protocol.

Eve the Eavesdropper

Eve is listening to the conversation between Peggy and Victor. A good zero-knowledge protocol also makes sure that any third-party will not learn a thing about the secret, and will not even be able to replay it for anyone else later to convince them.

Maggie the Malice

Maggie is listening to the protocol traffic and maliciously sending extra messages and modifying or destroying messages. The protocol must be tamper-resistant to this kind of activity. These names are used widely in this paper and elsewhere in the public key cryptography literature.

Zero-Knowledge Terminology

With Zero-knowledge protocols, the prover can convince the verifier that she is in possession of the knowledge, the secret, without revealing the secret itself, unlike e.g. normal username-password queries.

Often the prover will offer a *problem* (i.e. particular numeric values for a generic hard-to-solve mathematical problem, e.g. factoring extremely large numbers, which are products of large primes) to the verifier, which will ask for one of the 2 or more possible solutions. If the prover knows the real solution to the hard mathematical problem, she is able to provide any of the solutions asked for. If she doesn't know the real solution, she can not provide all of the possible solutions, and if the verifier asks for one of the other solutions, she is unable to provide it, and will be found out.

Because no information can leak from Peggy to Victor, Victor can't try to masquerade as Peggy to any outside third party. With some of these protocols, a man-in-the-middle attack is possible, though, meaning that someone can relay the traffic from the true Peggy and try to convince another Victor that he, the perpetrator, is Peggy. Also, if the verifier records the conversation between him and the prover, that recording can't be used to convince any third party. It looks the same as a faked conversation (e.g. where the verifier and prover agreed beforehand which requests the verifier will choose).

Modes of Operations

The zero-knowledge protocols can be used in three main modes.

Interactive: Where Peggy and Victor interactively go through the protocol, building up the certainty piece by piece.

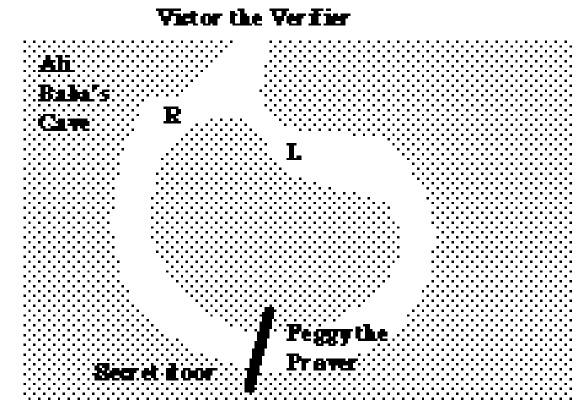
Parallel: Where Peggy creates a number of problems and Victor asks for a number of solutions at a time. This can be used to bring down the number of interactive messages with a slow-response-time connection.

Off Line: Where Peggy creates a number of problems, and then uses a cryptographically strong one-way hash function on the data and the set of problems to play the role of Victor, to select a random solution wanted for each problem. She then appends these solutions to the message. This mode can be used for *digital signatures* .

Example: Ali Baba's Cave

Consider the example of a circular variety of Ali Baba's cave shown in below Figure 2, with a

Figure: Example: Ali Baba's Cave



secret door that can be opened by a password. Peggy knows the password of the door, and wants to convince Victor that she knows it, but doesn't want Victor to know the password itself.

They work as follows:

- Peggy goes into a random branch of the cave, which Victor doesn't know standing outside the cave.
- Victor comes into the cave, and calls out a random branch of the cave (left or right), where Peggy should come out.
- If Peggy knows the secret password, she can come out the right way every time, opening and passing the secret door with the password if necessary. If Peggy doesn't know the password, she has a 50% chance of initially going into the wrong branch, and as she is not able to pass the secret door, Victor can call her bluff.

They repeat this as many times as needed to convince Victor. If Victor will be happy with a 1 in 1024 chance of Peggy not knowing the password, they need 10 repetitions (2^10 = 1024). This example also demonstrates another feature of zero-knowledge protocols: Now Victor is convinced that Peggy knows the secret password, but he cannot convince anyone else himself, as he doesn't know the secret!

Feige-flat-shamir Proof of Identity

This is the best-known zero-knowledge *proof of identity protocol* (Ivan Bjerre Damgård, 1989). A simplified version of this protocol works as follows (we present the full protocol here to give a taste of what most of these protocols look like. The rest will be handled in a more overviewing fashion):

- Precalculation: An arbitrator generates a random modulus *n* (512-1024 bits) which is the product of two large primes.The arbitrator generates a public and private key pair for Peggy, by choosing a number, *v*, which is a quadratic residue mod n (i.e. *x^2 = v mod n* has a solution, and *v^-1 mod n* exists). This number, *v* , is the public key. The private key is then the smallest *s* for which *s = sqrt(1/v) mod n*.
- The identification protocol proceeds then as follows: Peggy picks a random number *r* where *r<n*. She then computes *x = r^2 mod n* and sends it to Victor.
- Victor sends Peggy a random bit, *b.*
- If the bit is 0, Peggy sends Victor *r*. If the bit is 1, she sends *y = r * s mod n*.
- If the bit was 0, Victor verifies that *x = r^2 mod n,* proving that Peggy knows *sqrt(x).* If the bit was 1, he verifies that *x = y^2 * v mod n,* proving that Peggy knows *sqrt(x/v).*

If an impersonator tries to pass for Peggy, she can either pick *r* such that she can reply if Victor sends a 0 or 1 bit, but she cannot prepare for both cases, so she will be found out with a 50% chance each round.

Victor can't try to masquerade as Peggy to another verifier, as the bit Victor randomly sent to Peggy earlier has only a 50% chance of being the same as the second verifier will ask for. In this protocol, Peggy should never reuse an *r.* If she did, Victor could send her the other random bit, and collect a set of both responses. Then, if he had enough of these, he could try to impersonate Peggy to an outsider. This protocol can be implemented in a parallel fashion, making the public and private keys be a set of quadratic residues mod n, etc. Then you can do as many rounds in parallel as you have keys in the set, speeding up the protocol (but with larger memory requirements) and needing fewer messages.

Uillou-Quisquater proof identiy

This protocol is more suited to smart card applications, as it tries to keep the size of each accreditation[13] (i.e., each round) to a minimum. But it does require about 3 times the computational power of the Fiat-Shaumir protocol. This protocol requires that the prover have the following: A bit string of credentials *J* (card ID, validity, bank account number, ...) used as the public key, and application-specific pieces of public information, an exponent *v* and a modulus *n* , which is the product of two secret primes. The private key *B* is calculated so that *JB^v = 1 (mod n).* The protocol goes as follows:

- Peggy sends Victor her credentials *J*. She has to prove that the *J* are her credentials: She picks a random number *r*, so that 1 < *r* < *n*1. She sends *T = r^v (mod n)* to Victor.
- Victor picks a random number *d,* so that *0 < d <v1,* which he sends to Peggy.
- Peggy computes *D = rB^d (mod n)* and sends it to Victor.
- Victor computes *T' = D^v * J^d (mod n).* If *T = T' (mod n)* , then the authentication succeeds.

CONCLUSION

In this paper, we focus on the routing problem in delay tolerant networks in which nodes are disconnected most of the time and yet display a group behavior. We first propose a DTN network model representing an abstraction of node meetings in community-based networks. Then, we discuss the effects of distributing different number of copies to different communities on the performance of routing with the analysis of zero knowledge protocol proofing system.

It is evident from this study, that implementing real security does have quite large computational and memory requirements. So, in applications where good security is necessary, high-powered embedded controllers should be selected, so that they can work with the full-strength cryptographic protocols.

FUTURE WORK

As a fueture work, we will analyze the optimum distribution of copies to different communities. To this end, we would like to extend our fundamental analysis shown here to be applicable to many communities with various interaction rates between them by using zero knowledge Protocol.

REFERENCES

1. Bruce Schneier (1994), *Applied Cryptography*, Wiley & Sons, ISBN 0-471-59756-2.
2. Bulut E, Wang Z and Szymanski B (2008), *Time Dependent Message Spraying for Routing in Intermittently Connected Networks*, in Proceedings of Globecom 08, New Orleans, November.
3. BurgessJ, Gallagher B, Jensen D, and Levine B N (2006), *MaxProp: Routing for Vehicle-Based Disruption- Tolerant Networks*, In Proc. IEEE Infocom, April .
4. David Chaum (1987), Security without Identification: Card Computers to Make Big Brother Obsolete.
5. *Disruption Tolerant Networking*, http://www.darpa.mil/ato/solicit/DTN/.
6. Harras K, Almeroth K and Belding-Royer E (2005), *Delay Tolerant Mobile Networks*

(DTMNs): Controlled Flooding Schemes in Sparse Mobile Networks, In IFIP Networking, Waterloo, Canada, May.

7. Ivan Bjerre Damgård (1989), *Zero-Knowledge Protocols*, Århus University and CRYPTOMATHIC A/S.

8. Juang P, Oki H, Wang Y, Martonosi M, Peh L S and Rubenstein D (2002), *Energy-Efficient Computing For Wildlife Tracking: Design Tradeoffs And Early Experiences With Zebranet*, in Proceedings of ACM ASPLOS.

9. Lindgren A, Doria A and Schelen O (2003), "Probabilistic Routing in Intermittently Connected Networks", *SIGMOBILE Mobile Computing and Communication Review*, Vol. 7, No. 3.

10. Ott J and Kutscher D (2005), *A Disconnection-tolerant Transport For Drive-thru Internet Environments*, in Proceedings of IEEE INFOCOM.

11. Spyropoulos T, Psounis K and Raghavendra C S (2008), *Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-copy Case*, IEEE/ACM Transactions on Networking.

12. Spyropoulos T, Psounis K and Raghavendra C S (2005), *Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks*, ACM SIGCOMM Workshop.

13. Vahdat A and Becker D (2000), *Epidemic Routing for Partially Connected ad hoc Networks*, Duke University, Tech. Rep. CS-200006.

IJERST

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com

ISSN 2319-5991
01>
9 772319 599001