ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

High Throughput Multirouting in the Wireless network with path Metric computation

Anu S[1], Umarani R[2]

[1]Department Of Computer Science, Periyar University College Of Arts & Science,
Mettur Dam-01, Tamilnadu, India[1]

[2]Department Of Computer Science,Sri Saradha College For Women, Salem-16, Tamilnadu, India[2]

Abstract: Many applications and areas of wireless sensor networks (WSN), have diverse data traffic with different quality of service (QOS) requirements. As ddress the problem in this paper by Employing a High Throughput Metric (HTM), which finds high-throughput paths on multi-hop wireless networks. HTM minimizes the expected total number of packet transmissions (including retransmissions) required to successfully deliver a packet to the ultimate destination. In contrast, the minimum hop-count metric chooses arbitrarily among the different paths of the same minimum length, regardless of the often large differences in throughput among those paths, and ignoring the possibility that a longer path might offer higher throughput. This paper describes the design and implementation of HTM as a metric for the routing protocols. Experimental results demonstrate for long paths the throughput improvement is often a factor of two or more, suggesting that HTM will become more useful as networks grow larger and paths become longer.

Keywords: Wireless Sensor Networks, High Throughput, Quality of Service, Multirouting, path Estimation metric

I. INTRODUCTION

Multi-hop wireless mesh networks are composed of static nodes equipped with one or more radios that use each other to obtain network connectivity (through multi-hopping). Such networks have a variety of envisioned applications [1], [3]; the most important being the last-mile extension of the Internet in rural, underprivileged or underprovisioned neighborhoods. Challenges that routing and management protocols face in such networks stem from the vagaries of the wireless channel. This leads to the need to adapt and account for link dynamics due to fading, interference, obstacles etc. For example, distributed channel assignment algorithms typically periodically re-evaluate their assignment to deal with link dynamics. Routing protocols periodically probe the links to determine appropriate routes across the network. Networks with electronically steerable directional antennas may re- quire this information to reconfigure the network topology. Due to the complexity and inaccuracy of propagation and interference models, a link's performance is in practice typically characterized via some periodically measured link metric such as ETT (expected transmission time), ETX (expected transmission count), WCETT (weighted cumulative ETT), RTT (routing trip time), loss rate etc. While a lot of effort has been put into the design of link metrics; there has been little focus on the dynamics of these metrics, i.e. their stability and sensitivity. As a consequence, it is still not known how upper layer protocols should adapt to the link dynamics. Our study has practical significance since it uses two widely used and mature protocol implementations.

II. RELATED WORKS

The behavior of routing protocols over lossy links has been addressed and evaluated by real implementations in several papers. Chin et al. [8] also propose link handshaking to filter out asymmetric links. Hu and Johnson [14] describe how to preemptively issue DSR route requests, based on link SNR values. Yarvis et al. [05] observe that hop-count performs poorly as a routing metric for a sensor network, and present the results of using a loss-aware metric instead. Forward error correction, MAC-level acknowledgment and retransmission, and solutions such as Snoop-TCP [3] and Tulip [5] all take this approach. A number of existing ad hoc wireless routing algorithms collect per-link signal strength information and apply a threshold to avoid links with high loss ratios [8, 9, 10, 11, 14, 15,]. This approach may eliminate links that are necessary for connectivity, or fail to distinguish accurately between links; both of these are likely to be issues if many links have intermediate loss ratios.

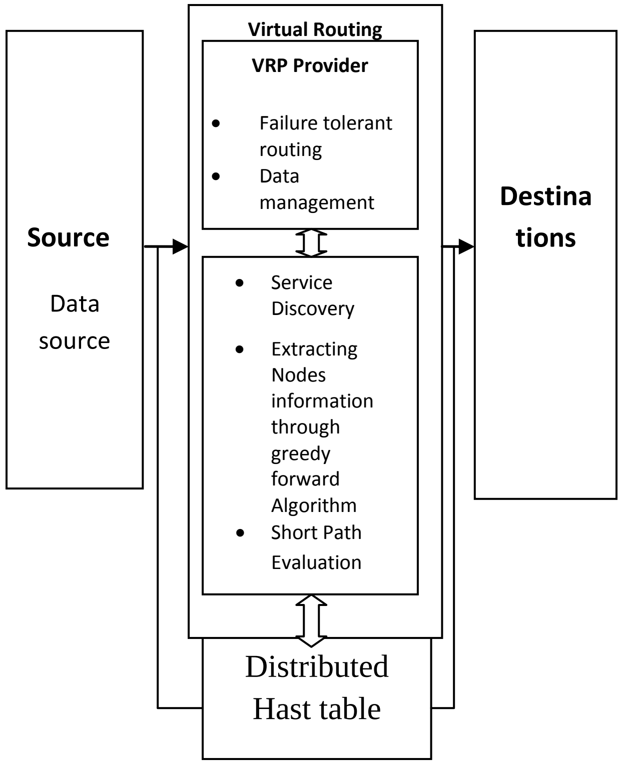
III. PROPOSED SYSTEM

A. Modeling the network entities

A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. This has been enabled by the availability, particularly in recent years, of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. The design of a WSN depends significantly on the application, and it must consider factors such as the environment, the application's design objectives, and cost, hardware, and system constraints. In general, WSNs provide an interesting research domain because they represent a class of massively distributed systems in which nodes are required to work in a cooperative and self-organized fashion to overcome scalability problems.

WSNs have changed from purely academic research test beds into real-world applications. Over the last decades, a wide variety of routing protocols has been developed in the domain of sensor networks. However, most practical approaches rely on standard Mobile Ad Hoc Network (MANET) protocols such as Ad Hoc on Demand Distance Vector (AODV), Dynamic MANET on Demand (DYMO), or Dynamic Source Routing (DSR).

IV. ARCHITECTURE DIAGRAM OF THE VIRTUAL ROUTING PROTOCOL USING HTM METRICS:



One of the major requirements in the domain of sensor networks is the need for network-centric operation. This property relies on the main working principles of WSNs, i.e., data are collected in a distributed way and need to be analyzed as close as possible to the data source. This working behavior saves communication and energy resources in sensor networks to a large extent.

V. EXPLORING HIGH THROUGHPUT PATHS BY DESIGNING THE HTM

Distributed Hash Tables (DHTs) are successfully used to distribute data over a large number of peers and to find optimal paths toward these data. The main idea is simple: Data items are associated with numbers and each node in the network is responsible for a range of these numbers. Therefore, it is easy to find the node at which a data item is stored. Usually, DHTs are built on the application layer and rely on an underlying routing protocol that provides connectivity between the nodes. A number of initial variables are initialized in the startup phase as listed in above Table. One node must be preprogrammed as initial node, i.e., it gets the position S.

VI. ALGORITHM FOR DEVELOPING HTM COMPUTATION FUNCTION

*Collect the Hop count with link loss ratio for HTM estimation for each route
*Per link delivery ratio has to be calculated
*End to end delivery probability has to be calculated for inter hop Interference dd
*Estimate the End to end delay ratio for the all routes dp
// Regular situation without any failures.
// Lookup the next hop to s in the primary lookup tables.
High throughput metrics = HTM= $\frac{1}{dr * df}$
// Node y has failed.
// Route m via alternate path c
// Intermediate destinations specified:
// already in failure recovery mode

VII. SHARING OF PATH METRIC BETWEEN ROUTES

The Effective path between each pair of nodes was found by sending data along ten potential best paths, one at a time, and selecting the path with the highest throughput. Potential best paths were identified by running an off-line routing algorithm, using as input measurements of per-link loss ratios.

VIII. SERVICE DISCOVERY BY EXTRACTING NODES INFORMATION THROUGH GREEDY FORWARD ALGORITHM

Routing in VCP is done using the virtual cord. Additionally, local neighborhood information is exploited for greedy routing. The greedy forwarding works as follows: a node with relative position P forwards a packet to its neighbor Ni that has the closest virtual position to the destination Dp. The forwarding is terminated if no more pr◀gress is possible, i.e., the local coordinate P is closest Dp. Based on the established cord, VRP routing will always lead to a path to the destination—it is not possible to run into a dead end.

IX. SHORTEST PATH EVALUATION FOR DATA TRANSMISSION

To improve the performance of greedy forwarding need to do process as follows. First, each node assigns itself an initial coordinate. Subsequently, nodes adjust their coordinates by simulating a system of springs and repulsion forces. Now, greedy routing is performed with only about 15 percent overhead compared to using real addresses. In the hop id routing scheme, each node maintains a hop id, which is a multidimensional coordinate based on the distance to some landmark nodes. In general, landmarks can be randomly selected in the network. However, to obtain better performance and to reduce the effect of dead ends, the authors present several methods for landmark selection.

X. FAILURE TOLERANT ROUTING AND DATA MANAGEMENT

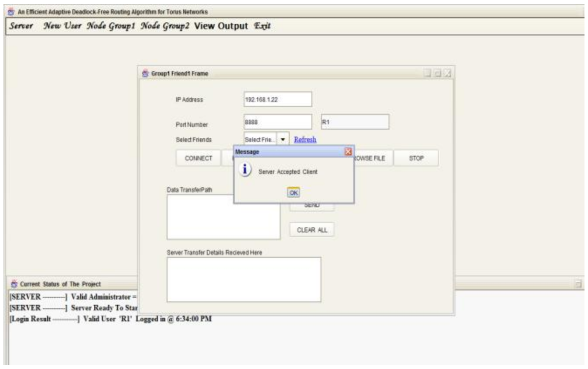
Virtual Routing Protocol (VCP) is an efficient, virtual relative position based routing protocol used in sensor networks. For ensuring an efficient and failure tolerant routing and data management, it exploits virtual coordinates in wireless networks. VRP maintains a virtual cord that interconnects all nodes in the sensor network. The operations of VRP are similar to a Distributed Hash Table (DHT). It provides the data managing support using DHT services. Moreover it supports service discovery using indirections.

XI. EXPERIMENTAL RESULTS:

A. *Simulation Setup.*

Thus implemented the proposed metric and routing procedure in data transmission in parallel computing in multiroute using the Gridsim simulator. simulate environments representative of mesh network deployments models environments with large trees and nodes where the designations is not in the line-of-sight of the sender's. The network consists of 100 nodes randomly placed. Randomly choose 20 nodes as multicast group members and one randomly selected node among them as the data source for desire action Attackers are randomly selected among nodes that are not group members. Group members join the group in the beginning of the simulation. At second 100, the source starts multicasting 512-byte data packets for 400 seconds at a rate of 20 packets/second.

Due to space constraint, do not present results for attacks that aim to cause large bandwidth overhead through frequent flooding of accusation messages using false accusations. The overhead of our defense consists of three components, the control bandwidth overhead due to additional messages and larger message size (e.g., accusation messages, signatures on query messages), the computational overhead due to cryptographic operations, and the additional data packet transmissions caused by our protocol.



IP Address 192.168.1.22
Port Number 8888 R1
Server Accepted Client
[SERVER --------] Valid Administrator =
[SERVER --------] Server Ready To Star
[Login Result --------] Valid User 'R1' Logged in @ 6:34:00 PM

Fig 1: Simulation Result of the Proposed functionality in Routing

XII. EFFECTIVENESS OF METRIC MANIPULATION ATTACKS

The impact of Drop-Only attack on the original VRP is measured through the HTM computation. The protocol is quite resilient to attacks, i.e., PDR decreases by only 15% for 20 attackers.

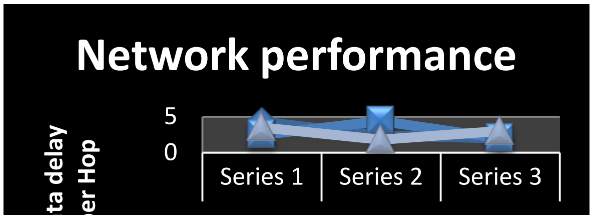


Fig 2: Network performance Via Data success ratio

This reflects the inherent resiliency of mesh based multicast protocols against packet dropping, as typically a node has multiple paths to receive the same packet. Thus, conclude that metric manipulation attacks pose a severe threat to high-throughput protocols.

XIII. EFFECTIVENESS OF THE DEFENSE

show the effectiveness of our defense gainst different types of attacks.

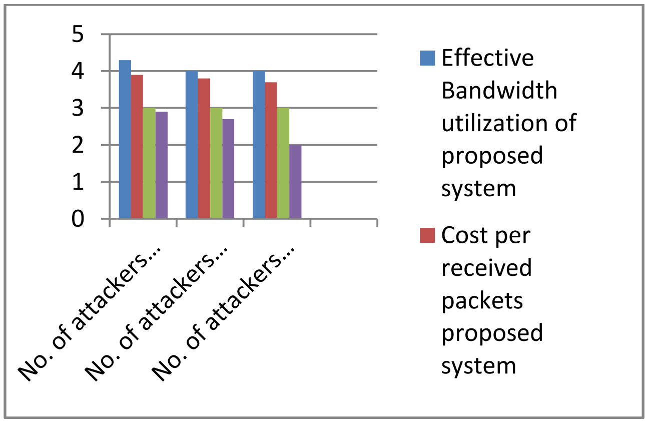


Fig 3: Experimental results for No. of traffics against Bandwidth and cost of packets utilized

For example, a total of 20 attackers cause a PDR drop of only 12%, considerably smaller than the case without defense, which shows a PDR decrease by as much as 55% in the GMM-Drop attack. To rule out random factors, performed a paired t-test on the results showing that VRP improves the PDR for all attack types. The small PDR decrease for VRP can be attributed to two main factors. First, common to all reactive schemes, attackers can cause some initial damage, before action is taken against them. Second, as the number of attackers increases, some receivers become completely isolated and are not able to receive data.

XIV. Defense Resiliency to Attacks

Attackers may attempt to exploit the accusation mechanism in VRP. Fig. shows that VRP is very resilient against the False-Accusation attack, in which attackers falsely accuse one of their neighbors. This comes from the controlled nature of accusations, which allows an attacker to accuse only one honest node at a time.

XV. Conclusion

Thus considered the security implication of using high throughput metrics in multicast protocols in wireless mesh networks. In particular, Thus identified metric manipulation attacks that can 14 inflict significant damage on the network. The attacks not only have a direct impact on the multicast service, but also raise additional challenges in defending against them due to their metric poisoning effect. Our defense also copes with transient network variations and malicious attempts to attack the network indirectly by exploiting the defense itself. Demonstrate through analysis and experiments that our defense is effective against the identified attacks, resilient to malicious Exploitations, and imposes a small overhead.

References

[1] J. Dong, R. Curtmola, and C. Nita-Rotaru, "On the pitfalls of using highthroughput multicast metrics in adversarial wireless mesh networks," in Proc. of IEEE SECON '08, 2008.

[2] Y. B. Ko and N. H. Vaidya, "Flooding-based geocasting protocols for mobile ad hoc networks," Mob. Netw. Appl., vol. 7, no. 6, 2002.

[3] R. Chandra, V. Ramasubramanian, and K. Birman, "Anonymous gossip: Improving multicast reliability in mobile ad-hoc networks," in ICDCS '01.

[4] Y.-B. Ko and N. H. Vaidya, "GeoTORA: a protocol for geocasting in mobile ad hoc networks," in Proc. of ICNP. IEEE, 2000, p. 240.

[5] E. L. Madruga and J. J. Garcia-Luna-Aceves, "Scalable multicasting: the core-assisted mesh protocol," Mob. Netw. Appl., vol. 6, no. 2, 2001.

[6] S. J. Lee, W. Su, and M. Gerla, "On-demand multicast routing protocol in multihop wireless mobile networks," Mob. Netw. Appl., 2002.

[7] E. M. Royer and C. E. Perkins, "Multicast ad-hoc on-demand distance vector (MAODV) routing," in Internet Draft, July 2000.

[8] J. G. Jetcheva and D. B. Johnson, "Adaptive demand-driven multicast routing in multi-hop wireless ad hoc networks." in MobiHoc, 2001.

[9] H. Lundgren, E. Nordstrom, and C. Tschudin, "Coping with communication gray zones in IEEE 802.11b based ad hoc networks," in WOWMOM '02.

[10] D. S. J. D. Couto, D. Aguayo, J. C. Bicket, and R. Morris, "A highthroughput path metric for multi-hop wireless routing," in MOBICOM '03.

[11] S. Roy, D. Koutsonikolas, S. Das, and C. Hu, "High-throughput multicast routing metrics in wireless mesh networks," in Proc. of ICDCS, 2006.

[12] A. Chen, D. Lee, G. Chandrasekaran, and P. Sinha, "HIMAC: High throughput MAC layer multicasting in wireless networks," in MASS '06.

[13] B. Awerbuch, D. Holmer, and H. Rubens, "The medium time metric: High throughput route selection in multirate ad hoc wireless networks," MONET, Spec. Iss. on Internet Wireless Access: 802.11 and Beyond, 2005.

[14] A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, "A multi-radio unification protocol for ieee 802.11 wireless networks," in BroadNets '04.

[15] S. Keshav, "A control-theoretic approach to flow control," Proc. of the Conference on Communications Architecture and Protocols, 1993.