Efficient Routing Protocol with Trust Management for Wireless Sensor Network –A Survey

Shilpa N[1], Dr. S. Ambareesh[2]
[1]PG Scholar, [2]Associate Professor
Department of Computer Science and Engineering
Vemana IT, Visvesvaraya Technological University, Belagavi, Karnataka, India.

***Abstract*—** **Wireless Sensor Network (WSN) is regarded as emerging futuristic technology which promises various applications development for military and people. Wireless Sensor Network technology is combined with processing power and wireless communications which makes it vulnerable for security breaches in the future. In addition of Wireless Technology it is open to all types of security threats. WSN is deal with both malicious and selfish misbehaving nodes. Our notion of selfishness is social selfishness as very often humans carrying communication devices (smart phones, GPSs, etc.) in a WSN are socially unselfish to friends but selfish to outsiders. Our notion of maliciousness refers to malicious nodes performing trust-related attacks to disrupt WSN operations built on trust (e.g., trust-based WSN routing considered in this project). We aim to design and validate a dynamic trust management protocol for WSN routing performance optimization in response to dynamically changing conditions such as the population of misbehaving nodes.**

Keywords- Wireless Sensor Network (WSN), Trust Management protocol, Delay/Disruption Tolerant Networks (DTNs).

I. INTRODUCTION

A Wireless Sensor Network (WSN) comprises mobile nodes (e.g., humans in a social WSN) experiencing opportunistic communication, sparse connection, and frequently changing network topology. This is because of lack of end-to-end connectivity, routing in WSN adopts a store carry-and-forward scheme by which messages are forwarded through a number of intermediate nodes leveraging opportunistic encountering, and hence resulting in high end-to-end latency. Here propose dynamic trust management for WSNs to deal with both malicious and selfish misbehaving nodes. The contributions of the relative to existing work in trust/reputation management for WSNs summarized as follows.

1. By proposing to combine social trust traditional Quality of Service (QoS) trust deriving from communication networks into a composite trust metric to assess the trust of a node in a WSN. To cope with both malicious and socially selfish nodes, here consider “healthiness” and “unselfishness” as two social trust metrics.

2. By proposing the notions of ‘objective trust’ vs. ‘subjective trust’ based on ground truth for protocol validation. For example, the healthiness trust of a good node should converge to 1 (ground truth) minus a false positive probability caused by noise, where the healthiness of a bad node should converge to 0 (ground truth) plus a false negative probability caused by noise and the random attack probability with which this bad node performs trust-related attacks.

3. Address the issue of application performance maximization (trust-based WSN routing) through dynamic trust management by adjusting trust aggregation or trust formation protocol settings dynamically in response to changing conditions to maximize WSN routing performance. Essentially address the importance of integration of trust and security metrics into routing and replication decisions in WSNs.

4. The develop of a novel model-based methodology utilizing Stochastic Petri Net (SPN) techniques [26] for the analysis of trust protocol and validate it via extensive real time. The model validated with real time yields actual ground truth node status against which “subjective” trust obtained from executing the trust protocol is verified, and helps in identifying the best protocol settings in response to dynamically changing network conditions to minimize trust bias and to maximize the routing application performance.

5. By performing a comparative analysis of trust-based WSN routing protocol built on top of dynamic trust management with real time validation against routing based on Bayesian trust management[12,14] (that is called Bayesian trust-based routing for short) and non-trust based (PROPHET [19] and epidemic[27]) protocols. The trust-based routing protocol outperforms Bayesian trust-based routing and PROPHET. Later, it approaches the ideal performance of epidemic routing in delivery ratio and message delay without incurring high message or protocol maintenance overhead.

II. RELATED WORK

A. *"To provide Social Trust by using Opportunistic Networks".*

Opportunistic networks enable mobile users to participate in various social interactions with applications such as content distribution and micro-blogs. Due to their distributed nature, securing user interactions depends rather on trust than hard cryptography. Trust is usually based on past user interactions such as in reputation systems relying on ratings. A more fundamental trust, social trust - assessing a user is genuine with honest intentions - must be established beforehand as many identities can be created easily (i.e., sybils). By leveraging the social network structure and its dynamics (conscious secure pairing and wireless contacts), by proposing the two complementary approaches for social trust establishment: explicit social trust and implicit social trust. Complexity, trust propagation and issues are evaluated using real world complex graphs, mobility traces and synthetic mobility models. To show how approach limits the maximum number.

B. *"Small World in Motion (SWIM): Modeling Communities in Ad-Hoc Mobile Networking".*

The complexity of social mobile networks, networks of devices carried by humans (e.g. PDAs or sensors) and communicating with short-range wireless technology, it makes hard protocol evaluation. We have a simple and efficient mobility model such as SWIM reflects correctly kernel properties of human movement and, at the same time, that allows to evaluate accurately protocols in this context. We need to investigate the properties of SWIM, to know how SWIM is able to generate social behavior among the nodes and how SWIM is able to model networks with a power-law exponential decay dichotomy of inter contact time and with complex sub-structures as the ones observed in the real data traces. Simulate three real scenarios and compare the synthetic data with real world data in terms of contact duration, inter-contact, number of contacts, and presence and structure of communities among nodes and find out a very good matching nodes. To compare the performance of BUBBLE, a community-based forwarding protocol for social mobile networks, on both real and synthetic data traces, to show that SWIM not only is able to extrapolate key properties of human mobility but also is very accurate in predicting performance of protocols based on social human sub-structures.

C. *"To Forward in Social Mobile Wireless Networks of Selfish Individuals".*

The present two forwarding protocols for mobile wireless networks of selfish individuals. Then assume that all the nodes are selfish and show formally that both protocols are strategy proof that is, none of the individual has an interest to deviate. An Extensive simulations with real traces show that the protocols introduce an extremely small overhead in terms of delay, while the techniques introduced to force faithful behavior have the positive and quite surprising side effect to improve performance by reducing the number of replicas and the storage requirements. To test the protocols also in the presence of a natural variation of the notion of selfishness-nodes that are selfish with outsiders and faithful with people from the same community. Even in this case, the protocols are shown to be very efficient in detecting possible misbehavior.

D. *RADON: reputation-assisted data forwarding in opportunistic networks".*

In opportunistic networks, the probability of encountering a destination node is popularly used to select a qualified forwarder; but it cannot represent the competency of delivering data in a hostile wireless environment. This is because a malicious node can bloat its probability to intercept data from others. The design of a reputation-based framework to more accurately evaluate an encounter's competency of delivering data, in such a way that it can be integrated with a large family of existing data forwarding protocols in opportunistic networks. Exactly a special message, called Positive Feedback Message (PFM), is proposed to help monitor the forwarding behavior of a node. Then also to design a Reputation-Assisted Data forwarding protocol for Opportunistic Networks (RADON), which integrates the reputation framework with a bare-bone data forwarding protocol using the number of times of previous encounters as the metric to select the next qualified forwarder. Through simulation experiments, to demonstrate that RADON effectively improves the network performance (e.g., data delivery ratio) against "black hole" attacks.

E. *"Trust Management for MANETs- A Survey".*

Managing trust in a distributed Mobile Ad Hoc Network (MANET) is challenging when collaboration or cooperation is critical to achieving mission and system goals such as reliability availability, re-configurability, and scalability. In defining and managing trust in a military MANET, should consider the interactions between the social, information, composite cognitive and communication networks, and it takes into account the severe resource constraints (e.g. computing power, energy, time, bandwidth), and dynamics (e.g., topology changes, node mobility, propagation channel conditions, node failure). It seek to combine the notions of "social trust" derived from social networks with "quality-of-service (QoS) trust" derived from information and communication networks to obtain a composite trust metric. Here the concepts and properties of trust and derive some unique characteristics of trust in MANETs drawing upon social notions of trust is discussed. Then provide a survey of trust management schemes developed for MANETs and discuss generally accepted classifications, trust metrics, and potential attacks performance metrics in MANETs. Finally, discuss of future research areas on trust management in MANETs based on the concept of social and cognitive networks is done

F. *"Trust Management in Ubiquitous Computing: A Bayesian Approach".*

Designing a trust management scheme that can effectively evaluate the relationships among devices in pervasive computing environments is a challenging task. Here it continues the investigation of the recently proposed probabilistic trust management scheme for pervasive computing environments. Then argue that in addition to allowing a device to find other appropriate devices with which to interact, at the same time it detects those that are malicious, the trust management scheme is also capable of (1) allowing a device to judge the trustworthiness of another device it interacts with, while it makes a better use of the received recommendations and (2) behaving as expected when a device has little or enough experience of interactions with other devices and changes dynamically occurs in the proportion of malicious devices. Then the simulation experiments are provided to assess the achievement of the stated goals, by using some representative performance metrics.

G. *"Networking Named Content".*

Network use has evolved to be dominated by content distribution and retrieval, while networking technology still speaks only of connections between hosts. In order to access content and services requires mapping from the users care about to the network's where. To present Content-Centric Networking (CCN) which treats content as a primitive - decoupling location from identity, security and access, and retrieving content by name. Using new approaches to routing named content, derived heavily from IP, it can simultaneously achieve scalability, security and performance. So it is implemented the architecture's basic features and demonstrate resilience and performance with secure file downloads and VoIP calls.

H. *"An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks".*

Delay/Disruption Tolerant Networks (DTNs) have been identified as one of the key areas in the field of wireless communication, wherein delay and sparseness are particularly high. They are rising as a promising technology in planetary/interplanetary, vehicular, military/tactical, disaster response, satellite and underwater networks. DTNs are characterized by large end-to-end communication latency and the lack of end-to-end path from a source to its destination. These characteristics to present several challenges to the security of DTNs. In particular, Byzantine attacks in which one or more legitimate nodes have been compromised and fully controlled by the adversary can give serious damages to the network in terms of data availability and latency. Using reputation-based trust management systems is shown to be an effective way to handle the adversarial behavior in Mobile Ad hoc Networks (MANETs). However, because of the unique characteristics of DTNs, some of those traditional techniques do not apply to DTNs. The main objective is to develop a robust trust mechanism and an efficient and low cost malicious node detection technique for DTNs. Inspired by the recent results on reputation management for online systems and e-commerce, so develop an iterative malicious node detection mechanism for DTNs referred as ITRM. Then the proposed scheme is a graph-based iterative algorithm motivated by the prior success of message passing techniques for decoding low-density parity-check codes over bipartite graphs. By applying ITRM to DTNs for various mobility models, here observed that the proposed iterative reputation management scheme is far more effective than well-known reputation management techniques such as the Bayesian framework and Eigen Trust. Further, concluded that the proposed scheme provides high data availability and packet-delivery ratio with low latency in DTNs under various adversary attacks which attempt to both undermine the trust and detection scheme and the packet delivery protocol.

III. SYSTEM DESIGN

We are considering a Delay Tolerant Network environment with no centralized trusted authority. Nodes communicate through multiple hops. When a node encounters another node, at that time they will exchange encounter histories and this encountered histories are certified by encounter tickets [16] so as to prevent black hole attacks to DTN routing. We differentiate socially selfish nodes from malicious nodes. A selfish node may acts for its own interests including interests to its friends, communities, or groups. So it may drop packets randomly just to save energy but it may decide to forward a packet if it has good social ties with the source (sender), current carrier or destination node.

We consider a friendship matrix [18] to represent the social ties among nodes. Here each node will maintain a friend list in its local storage. A same concept to the friendship relationship is proposed in [20], where familiar strangers are identified based on collocation information in dense populated area transport environments for media sharing. Our work is different from [20] in that rather than by frequent collocation instances, friendship is established by the existence of common friends. Energy spent for maintaining the friend lists and performing required operations is very negligible because the energy spent for computation is very small compared with that for Delay Tolerant Network communication and matching operations are performed only when any changes made in the friend lists. When a node becomes selfish, at that time it will only forward messages when it is a friend of the source, current carrier, or the destination (receiver) node, whereas well-behaved node performs selflessly regardless of the social ties. A malicious node aims to break the basic DTN routing functionality. In addition to dropping packets, a malicious node can perform the trust-related attacks such as:

1. Self-promoting attacks: it can promote its importance (this is done by providing very good influence for itself) so as to attract packets routing through it (and being dropped).

2. Bad-mouthing attacks: it can ruin the reputation of well-behaved nodes (this is done by providing bad influence against good nodes) so as to decrease the chance of packets routing through well behaved nodes.

The system architecture (figure 1) consists of the following system entities.

1) Source: Source will send the data to destination through level 1 and level 2 routers each level contains the four nodes, before sending the data source will check the healthiness of the nodes and the connectivity. Healthiness of node is nothing

but the combination of Trust Percentage and Energy Percentage of a respective node.

2) Trust Level Optimization: In level 1 Source will select next hop node which is having more nodes weight that respective node will be selected as a Next Hop Node. Level 1 will select the next hop node from level 2 nodes. Before selecting Level 1 will check the Node weight of each node. In level 2 has to receive the file from level 1 and transfer to the file to destination and destination has to give the acknowledgement to the level 2.

3) Attacker Module: In attacker module different kinds of attack such as Self-promoting attacks etc. Ballot stuffing it can boost the reputation of bad nodes (by providing good recommendations for them) so as to increase the chance of packets routing through malicious nodes (and being dropped). Attacker will happen in between the levels of nodes if any kind of attack once attack happens node does not send the data as well as acknowledge.

4) Destination: Destination will receive the data and send acknowledge to level 2 routers and level 2 forward the acknowledge to the level 1 routers finally level 1 forward the acknowledge to source.

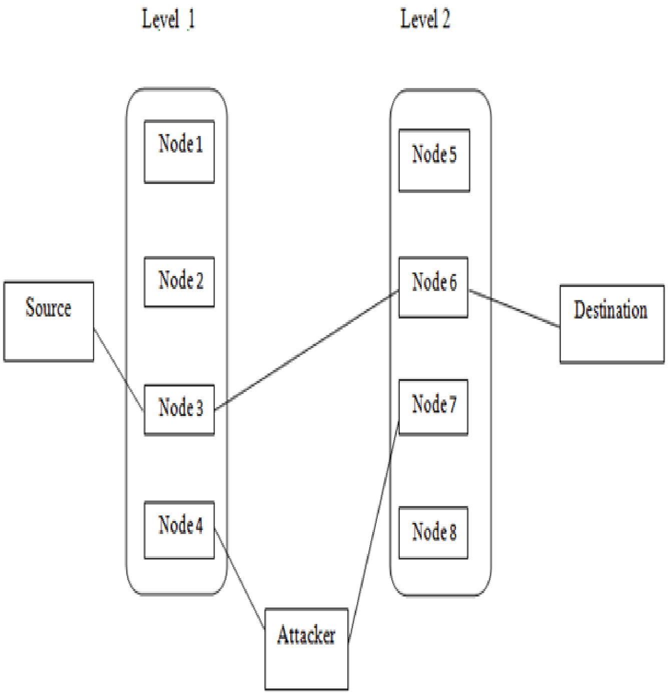

Figure 1: System architecture

ALGORITHMS USED

1. Next – Hop Select Pseudo Code:

```
➢ Node M wants to select his next hop Node to transfer the DATA
➢ Let N is No of Nodes Available in next Hop
➢ Initialize array T [ N ]
    • For I = 1 to  N
    • Get the distance, energy, trust, connection details of Node I
    • Calculate the weight of  Node I based on parameter
    • A [ I ] = weightage
    • Next I
➢ Find the Node with highest weightage
➢ Shortlist the Node ( k ) which has highest weightage
➢ Transfer the DATA  to Node k
```

2. Trust Calculation of Node Pseudo Code

```
➢ Generate the Trust parameter results for each node in the nodes list.
➢ I.e. trust parameters are Distance, Energy, Trust, and Connectivity.
    • Assume Distance=7 then 100-7=93 i.e, 93 is Distance value of node.
    • Energy = 90,
    • Trust Value= $\frac{\text{No. of ack received}}{\text{(Total packets sent)}} X 100$
    • Connectivity=3 , then 3 X 10 =30. Connectivity value is 30.
➢ Total NodeWeight = $\frac{\text{Distance +Energy +Trust+ Connectivity}}{4}$
➢ Which node is having the highest node weight that node is trustful node in the nodes list.
```

CONCLUSION

In this paper, we designed and validated a trust management protocol for DTNs and it is applied it to demonstrate its utility in secure routing. Our trust management protocol merges QoS trust with social trust to obtain a composite trust metric. Our design permits the best trust setting for trust aggregation to be identified so that subjective trust is closest to objective trust for each individual trust property for minimizing trust bias. Further, our design also permits application performance. Here we demonstrated how the results obtained at design time can facilitate dynamic trust management for DTN routing in response to dynamically changing conditions at runtime. We performed a comparative analysis of trust-based secure routing running on top of our trust management protocol with Bayesian trust-based routing and non-trust-based routing protocols (epidemic and PROPHET) in DTNs. Our results backed by simulation validation demonstrate that our trust-based secure routing protocol outperforms PROPHET and Bayesian trust-based routing. Further, it approaches the ideal performance of epidemic routing in delivery ratio and message delay without incurring high message or protocol maintenance overhead.

There are several research areas in future including (a) exploring other trust-based DTN applications with which we could further demonstrate the utility of our dynamic trust management protocol design; (b)designing trust management for DTNs considering social communities and performing comparative analysis with more recent works such as [2, 3]; (c) implementing our proposed dynamic trust management protocol on top of a real DTN architecture [5] to further validate the protocol design, as well as to quantify the protocol overhead; (d) investigating trust-based admission control strategies as in [7-9] used by selfish nodes to maximize their own payoffs while contributing to DTN routing performance; and (e) developing trust and security management protocols for delay-tolerant, self-contained message forwarding applications based on the information-centric networks (ICN) architecture [13].

REFERENCES

[1] The ns-3 Network Simulator, Nov. 2011, http://www.nsnam.org/.

[2] E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks," *Military Communications Conference*, 2010, pp. 1788-1793.

[3] E. Ayday, H. Lee, and F. Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay Tolerant Networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 9, Sept. 2012, pp. 1514-1531.

[4] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networking," *IEEE Conference on Computer Communications*, Barcelona, Spain, April 2006, pp. 1-11.

[5] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture," *RFC 4838*, IETF, 2007.

[6] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Supplemental Material for 'Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing'," *IEEE Transactions on Parallel and Distributed Systems*, 2013. . Chen, and T. H. Hsi, "Performance Analysis of Admission Control Algorithms Based on Reward Optimization for Real-Time Multimedia Servers," *Performance Evaluation*, vol. 33, no. 2, 1998, pp. 89-112.

[7] S. T. Cheng, C. M. Chen, and I. R. Chen, "Dynamic Quota-Based Admission Control with Sub-Rating in Multimedia Servers," *Multimedia Systems*, vol. 8, no. 2, 2000, pp. 83-91.

[8] S. T. Cheng, C. M. Chen, and I. R. Chen, "Performance Evaluation of an Admission Control Algorithm: Dynamic Threshold with Negotiation," *Performance Evaluation*, vol. 52, no. 1, 2003, pp. 1-13.

[9] J. H. Cho, A. Swami, and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, 2011, pp. 562-583.

[10] E. M. Daly, and M. Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs," *IEEE Transactions on Mobile Computing*, vol. 8, no. 5, May 2009, pp. 606-621.

[11] M. K. Denko, T. Sun, and I. Woungang, "Trust Management in Ubiquitous Computing: A Bayesian Approach," *Computer Communications*, vol. 34, no. 3, 2011, pp. 398-406.

[12] V. Jacobson, D. K. Smetters, J. D. Thornton, M. Plass, N. Briggs, and R. Braynard, "Networking Named Content," *Communications of the ACM*, vol. 55, no. 1, 2012, pp. 117-124.

[13] A. Jøsang, and R. Ismail, "The Beta Reputation System," *Bled Electronic Commerce Conference*, Bled, Slovenia, June 17-19 2002, pp. 1-14.

[14] S. Kosta, A. Mei, and J. Stefa, "Small World in Motion (SWIM): Modeling Communities in Ad-Hoc Mobile Networking," *7th IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, Boston, MA, USA, June 2010.

[15] F. Li, J. Wu, and A. Srinivasan, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks using Encounter Tickets," *IEEE Conference on Computer Communications*, 2009, pp. 2428-2436.

[16] N. Li, and S. K. Das, "RADON: Reputation-Assisted Data Forwarding in Opportunistic Networks," *2nd ACM International Workshop on Mobile Opportunistic Networking*, Pisa, Italy, Nov. 2010, pp. 8-14.

[17] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," *IEEE Conference on Computer Communications*, San Diego, CA, March 2010, pp. 1-9.

[18] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, 2003, pp. 19-20.

[19] L. McNamara, C. Mascolo, and L. Capra, "Media Sharing based on Colocation Prediction in Urban Transport," *14th Annual International Conference on Mobile Computing and Networking*, San Francisco, CA, USA, 2008.

[20] A. Mei, and J. Stefa, "Give2Get: Forwarding in Social Mobile Wireless Networks of Selfish Individuals," *IEEE International Conference on Distributed Computing Systems*, Genoa, Italy, June 2010, pp. 488-297.