World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 253-258, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.csea.2247

Cooperative Trust Management Scheme for Wireless Sensor Networks

K.P. Thooyamani, R. Udayakumar and V. Khanaa

Professor School of Computing Science, Bharath University, Chennai-73 India

Abstract: This document presents a trust management scheme which is based on direct and indirect interactions with neighboring nodes, to compute their trust value and thus select the most trusted path or forwarding node. This trust framework enables us to detect malicious nodes. Also this will employ less consumption of resources namely memory and power. AODV Communication protocol is made use in this scheme in order to achieve efficient dissemination of information among sensors as an energy-conserving form of communication. This scheme holds a typical application that lies in military situations where the nodes can self-organize themselves and provide unattended monitoring of the deployed area by gathering information about an event and rely this information back to friendly base station for further processing and decision making.

Key words: Wireless Sensor Networks · Trust Evaluation · Trust Modeling · Malicious Nodes · AODV Protocol.

INTRODUCTION

Advances in the miniaturization of micro-electro-mechanical systems have led to extremely small, battery-powered sensing devices that have sensing, communication and processing capabilities. These sensor nodes can be networked in an ad hoc manner to perform distributed sensing and information processing. These networks can be deployed in inhospitable terrains or in hostile environments to provide continuous monitoring and processing capabilities. Such kind of systems need good amount of accuracy. To incorporate this appropriate Trust Modeling and Trust evaluation is required to judge the quality of sensor nodes and their services. Also, to provide reliable routing path that does not contain any malicious nodes. In this project, memory is conserved by representing the trust value within the range 0 to 100 rather than representing in the range -1 to 1. Also power is saved by bring out a new expression for trust value calculation as the traditional method of calculating trust consumes much of clock cycles which in turn increases power consumption. Main aim of our project is to reduce the memory usage and power consumption Our proposed system will calculate the trust value based on direct or indirect observations. Direct trust is the value that indicates the trust that node A builds progressively for node B, utilizing its own routing experience (direct interactions). We denote as DT (A, B) the direct trust value that A has built for node B based on a set of events. Direct observation represents the number of successful and unsuccessful interactions. Indirect Trust value indicate the trust that node A builds for node B based on the reputations provided by neighboring nodes. We denote as IT(A,B) the indirect trust value that A calculates for neighboring node B.

Successful Interaction: Sender consider an interaction to be successful if the sender receives an assurance that the packet is successfully received by the Neighbor node and that node has forwarded the packet towards the destination in an unaltered fashion. Thus The first requirement *i.e*., successful reception, is achieved on reception of the link layer acknowledgement [1]. IEEE 802.11 is a standard link layer protocol which is discussed in the next section. The second requirement, i.e., forwarding of the packet, is achieved by using enhanced passive acknowledgment by overhearing the transmission of a next hop on the route, since they are within the radio range. Another parameter for calculating Trust i.e., Unsuccessful interaction description is shown in the next sub section.

Corresponding Author: K.P. Thooyamani, Professor School of Computing Science, Bharath University, Chennai-73 india.

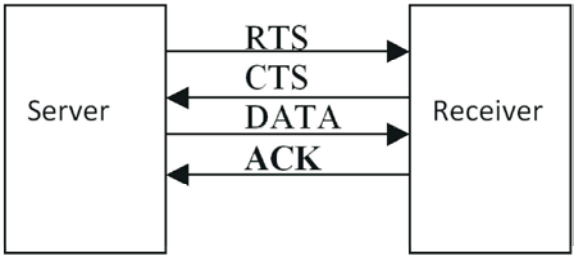

Fig. 1: Four way Handshake methodology

Unsuccessful Interaction: If a node does not forward a packet or modifies & send the packet then such node is called as malicious node which leads to unsuccessful interaction[2]. This is referred in detail with reference to the IEEE 803.11 in the next section.

WPAN-IEEE 802.15.4 Standard Link Layer MAC Protocol: Data transmission happens based on the IEEE 802.11 standard link layer MAC protocol. This involves four way handshake methodologies as shown in fig. 1 whose steps are listed below:

- Sender sends Ready-to-Send (RTS)
- Receiver responds with Clear-to-Send (CTS)
- Sender sends DATA PACKET
- Receiver acknowledge with ACK
- RTS and CTS announce the duration of the transfer
- Nodes overhearing RTS/CTS keep quiet for that duration
- Sender will retransmit RTS if no ACK is received

Thus when the sender receives ACK signal from receiver then it can assure that successful transmission has occurred. If ACK is sent out, but not received by sender, after receiving new RTS, receiver returns ACK instead of CTS for new RTS. If the sensor node does not overhear the retransmission of the packet within a threshold time from its neighboring node or the overheard packet is found is to be illegally fabricated, then the sensor node will consider that interaction as an unsuccessful one. If the number of unsuccessful interactions increases, the sender node decreases the trust value of that neighboring node and may consider it as a malicious node.

Trust: Trust in general is the level of confidence in a person or a thing. Various engineering models such as security, usability, reliability, availability, safety and privacy models incorporate some limited aspects of trust with different meanings. For example, in sensor network security, trust is a level of assurance about a key's authenticity that would be provided by some centralized trusted body to the sensor node (SN).In wireless ad hoc and sensor network reliability, trust is used as a measure of node's competence in providing required service[3-6]. In general, establishing trust in a network gives many benefits such as the following:

- Trust solves the problem of providing corresponding access control based on judging the quality of SNs and their services. This problem cannot be solved through traditional security mechanisms.
- Trust solves the problem of providing reliable routing paths that do not contain any malicious, selfish, or faulty node(s) .
- Trust makes the traditional security services more robust and reliable by ensuring that all the communicating nodes are trusted during authentication, authorization, or key management .

A number of trust management schemes have been proposed for peer-to-peer networks and ad hoc networks . To the best of our knowledge, very few comprehensive trust management schemes (e.g., Reputation-based Framework for Sensor Networks (RFSN), Agent-based Trust and Reputation Management (ATRM) and Parameterized and Localized trust management Scheme (PLUS) have been proposed for sensor networks. Although, there are some other works available in the literature that discuss trust but not in much detail. Within such comprehensive works, only ATRM scheme is specifically developed for the clustered WSNs. However, this and other schemes suffer from various limitations such as these schemes do not meet the resource constraint requirements of the WSNs and, more specifically, for the large-scale WSNs. Also, these schemes suffer from higher cost associated with trust evaluation especially of distant nodes. Furthermore, existing schemes have some other limitations such as dependence on specific routing scheme, like PLUS works on the top of the PLUS_R routing scheme; dependence on specific platform, like the ATRM scheme requires an agent-based platform; and unrealistic assumptions, like the ATRM assumes that agents are resilient against any security threats and so forth. Therefore, these works are not well suited for realistic WSN applications. Thus, a lightweight secure trust management scheme is needed to address these issues.

Related Work: Research work on trust management schemes for WSNs is in its infancy. To our knowledge, very few trust management schemes have been proposed

such as RFSN, ATRM and PLUS. Trust values are calculated on the basis of that reputation and they use Bayesian formulation for representing reputation of a node. RFSN assumes that the node has enough interactions with the neighbors so that the reputation (beta distribution) can reach a stationary state. However, if the rate of node mobility is higher, reputation information will not stabilize. In RFSN, no node is allowed to disseminate bad reputation information. If it is assumed that "bad" reputation is implicitly included by not giving out good reputation, then in that case, the scheme will not be able to cope with uncertain situations.

Boukerche *et al*. have proposed an ATRM scheme for WSNs. ATRM is based on a clustered WSN and calculates trust in a fully distributed manner. ATRM works on specific agent-based platform. Also, it assumes that there is a single trusted authority, which is responsible for generating and launching mobile agents, which makes it vulnerable against a single point of failure. ATRM also assumes that mobile agents are resilient against malicious nodes that try to steal or modify information carried by the agent. In many applications, this assumption may not be realistic.

Yao *et al* have proposed PLUS for sensor network security. The authors adopt a localized distributed approach and trust is calculated based on either direct or indirect observations. This scheme works on top of their own defined routing scheme called PLUS_R. In this scheme, the authors assume that all the important control packets generated by the BS must contain a hashed sequence number (HSN). Inclusion of HSN in control packets not only increases the size of packets resulting in higher consumption of transmission and reception power but also increases the computational cost at the SNs. whenever a judge node receives a packet from another node i, it will always check the integrity of the packet. If the integrity check fails, then the trust value of node i will be decreased irrespective of whether node i was really involved in maliciously making some modification in a packet or not. So, node i may get unfair penalty.

Recently, Liu et al have proposed a very simple trust management scheme for Resilient Geographic Routing (T-RGR). Their trust algorithm works in a fully distributed manner, in which each node monitors the behavior of one-hop neighbors. In the T-RGR scheme, authors have used many predefined threshold values that make their scheme non adaptive. Also, in their scheme, each node only relies on its direct monitoring for calculating trust value, which makes it vulnerable against collaborative attacks.

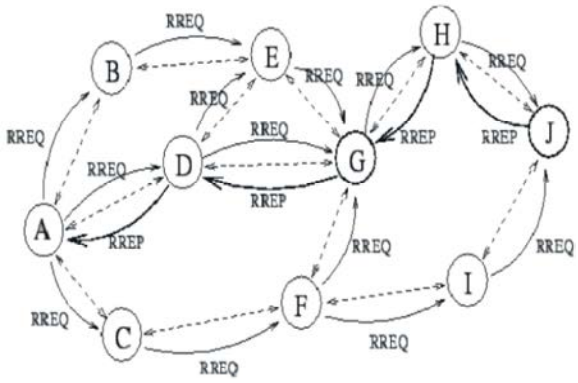

Fig. 2: Example of an AODV path discovery.

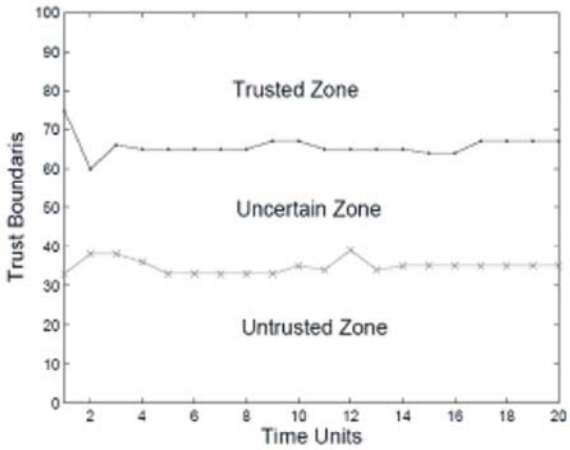

Fig. 3: Trust value classification

Ad-Hoc On-Demand Vector (AODV): AODV is a relative of the Bellmann-Ford distant vector algorithm, but is adapted to work in a mobile environment. AODV determines a route to a destination only when a node wants to send a packet to that destination. Routes are maintained as long as they are needed by the source. Sequence numbers ensure the freshness of routes and guarantee the loop-free routing. Path discovery in this AODV is done using Route request (RREQ) and route reply (RREP) [7-10].This mechanism is illustrated in fig. 2.

AODV uses symmetric links between neighboring nodes. It does not attempt to follow paths between nodes when one of the nodes cannot hear the other one; however we may include theuse of such links in future enhancements.

The Ad-Hoc On-Demand Distance Vector Algorithm: Our basic proposal can be called a pure on-demand route acquisition system; nodes that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further, a node does not have to discover and maintain a route to another

node until the two need to communicate, unless the former node is offering its services as an intermediate forwarding station to maintain connectivity between two other nodes.

When the local connectivity of the mobile node is of interest, each mobile node can become aware of the other nodes in its neighborhood by the use of several techniques, including local (not system-wide) broadcasts known as hello messages. The routing tables of the nodes within the neighborhood are organized to optimize response time to local movements and provide quick response time for requests for establishment of new routes. The algorithm's primary objectives are:

- To broadcast discovery packets only when necessary
- To distinguish between local connectivity management (neighborhood detection) and general topology maintenance
- To disseminate information about changes in local connectivity to those neighboring mobile nodes that are likely to need the information[11].

Path Discovery: The Path Discovery process is initiated whenever a source node needs to communicate with another node for which it has no routing information in its table. Every node maintains two separate counters: a node sequence number and a broadcast-id. The source node initiates path discovery by broadcasting a route request (RREQ) packet to its neighbors. The RREQ contains the following fields:

< source_addr, source sequence^, broadcast Id, dest-addr, destsequencehop-cnt >

The pair < source.addr, broadcast Id > uniquely identifies a RREQ. Broadcast Id is incremented whenever the source issues a new RREQ. Each neighbor either satisfies the RREQ by sending a route reply (RREP) back to the source or re-broadcasts the RREQ to its own neighbors after increasing the hop-cnt. Notice that a node may receive multiple copies of the same route broadcast packet from various neighbors. When an intermediate node receives a RREQ, if it has already received a RREQ with the same broadcast Id and source address, it drops the redundant RREQ and does not rebroadcast it. If a node cannot satisfy the RREQ, it keeps track of the following information in order to implement the reverse path setup, as well as the forward path setup that will accompany the transmission of the eventual RREP:

- Destination IP address
- Source IP address
- Broadcast Id
- Expiration time for reverse path route entry
- Source node's sequence number.

Reverse Path Setup: There are two sequence numbers (in addition to the broadcast Id) included in a RREQ: the source sequence number and the last destination sequence number known to the source. The source sequence number is used to maintain freshness information about the reverse route to the source and the destination sequence number specifies how fresh a route to the destination must be before it can be accepted by the source[12].

As the RREQ travels from a source to various destinations, it automatically sets up the reverse path from all nodes back to the source [4], as illustrated in Figure 1. To set up a reverse path, a node records the address of the neighbor from which it received the first copy of the RREQ. These reverse path route entries are maintained for at least enough time for the RREQ to traverse the network and produce a reply to the sender.

Forward Path Setup: Eventually, a RREQ will arrive at a node (possibly the destination itself) that possesses a current route to the destination. The receiving node first checks that the RREQ was received over a bi-directional link. If an intermediate node has a route entry for the desired destination, it determines whether the route is current by comparing the destination sequence number in its own route entry to the destination sequence number in the RREQ. If the RREQ's sequence number for the destination is greater than that recorded by the intermediate node, the intermediate node must not use its recorded route to respond to the RREQ. Instead, the intermediate node rebroadcasts the RREQ. The intermediate node can reply only when it has a route with a sequence number that is greater than or equal to that contained in the RREQ. If it does have a current route to the destination and if the RREQ has not been processed previously, the node then unicasts a route reply packet (RREP) back to its neighbor from which it received the RREQ. A RREP contains the following information:

<source-addr, dest_addr, destsequence hop-cnt, lifetime>

By the time a broadcast packet arrives at a node that can supply a route to the destination, a reverse path has been established to the source of the RREQ (Section 2.1.1). As the RREP travels back to the source, each node

along the path sets up a forward pointer to the node from which the RREP came, updates its timeout information for route entries to the source and destination and records the latest destination sequence number for the requested destination. Figure 2 represents the forward path setup as the RREP travels from the destination D to the source node S. Nodes that are not along the path determined by the RREP will timeout after AC-TIVE_ROUTE_TIMEOUT (3000msec) and will delete the reverse pointers.

A node receiving an RREP propagates the first RREP for a given source node towards that source. If it receives further RREPs, it updates its routing information and propagates the RREP only if the RREP contains either a greater destination sequence number than the previous RREP, or the same destination sequence number with a smaller hop count. It suppresses all other RREPs it receives. This decreases the number of RREPs propagating towards the source while also ensuring the most up-to-date and quickest routing information. The source node can begin data transmission as soon as the first RREP is received and can later update its routing information if it learns of a better route.

Representation of Trust Values: Generally, a trust value is considered to be a numerical quantity lying between 0 and 1 (inclusive) as suggested earlier or between-1 and 1 (inclusive) on a real number line. In this paper, we use trust value as an integer in the interval between 0 and 100 (inclusive)[13]. However, other ranges, for example base 2 ranges, could be used as well. Although presenting the trust values as a real number or integer may not play an important role in traditional networks, but for SNs this issue is of critical importance due to limited memory and transmission, reception power. This change will give us benefits such as: Representation of trust value [0, 100] as an unsigned integer (1 byte) saves 75 percent of memory space as compared to trust values represented as a real number (4 bytes). Less number of bits need to be transmitted during the exchange of trust values between SNs. This gives us the benefit of less consumption of transmission and also the reception power [14].

Thus the least trust valued node is detected as the malicious node. By this way we can detect the malicious node and thus select the most trusted path or forwarding node.

Simulation Analysis and Evaluation

Simulation Environment: Simulation has been done using the Network Simulator-2 (NS-2).We have deployed 60 nodes ranging from 0 to 59.The WSN topology used in the simulation scenarios is shown in the figure 4.

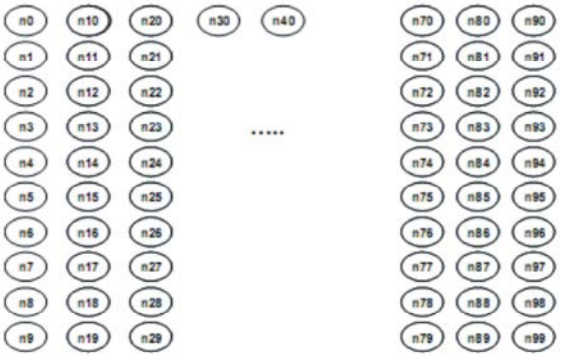

Fig. 4: Layout used in the WSN topology for communicating between nodes about Trust

The objective of AODV protocol used in our network is to exchange the Trust values between communicating nodes in an efficient manner.

Using the evaluation from the Network simulator-2, now it is possible for us to fetch few important constraints like packet delivery ratio, end-to-end delay, number of packets sent, forwarded and acknowledged successfully. It is observed that these values are appreciatable when compared to other protocols used traditionally.

CONCLUSION

Cooperative Trust Management Schemes been shown to detect fast malicious nodes and reacts in their detection, finding alternative paths. As soon as the malicious nodes are detected, the network performance becomes identical to the one observed for no malicious nodes in the network. Additionally, its power and memory consumption. Cooperative Trust Management Scheme is suitable for large wireless sensor networks while at the same time, node and network resources are economized. The simulation results show that significant power and energy is consumed for routing and trust purposes. This scheme guides the sensor nodes select for forwarding the neighbor that is not only closer to the destination but also has enough remaining energy, leading to an efficient scheme.

REFERENCES

1. Giruka, V.C., M. Singhal, J. Royalty and S. Varanasi, 2008. ecurity in wireless sensor networks", Wireless Communications & mobile Computing, 8: 1-24.
2. Kannhavong, B., H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, 2007. "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless Communications, 14(5): 85-91.

3. Karlof, C. and D. Wagner, 2003. "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", IEEE International Workshop on Sensor Network Protocols and Applications, pp: 113-127.
4. Li, H. and M. Singhal, 2006. "A Secure Routing Protocol for Wireless ad hoc Networks", Int. Conference on system Sciences, Hawaii, pp: 4-7.
5. Rezgui, A. and M. Eltoweissy 2007. "TARP: A Trust-Aware Routing Protocol for Sensor-Actuator Networks" IEEE International Conference on Mobile Ad hoc and Sensor Systems, MASS, Pisa, Italy.
6. Junbeom Hur, Younho Lee, Hyunsoo Yoon, Daeseon Choi and Seunghun Jin, 2005. "Trust evaluation model for wireless sensor networks" Advanced Communication Technology Conference, ICACT, pp: 491-496
7. Sapon Tanachaiwiwat, Pinalkumar Dave, Rohan Bhindwale and Ahmed Helmy 2004. "Location-centric Isolation of Misbehavior and Trust Routing in Energy-constrained Sensor Networks" IEEE International Conference on Performance, Computing and Communications.
8. Pirzada, A.A. and C. McDonald, "Trust Establishment In Pure Ad-hoc Networks", Wireless Personal Communications, 37: 139-163.
9. Jeng-Wei Lee, Yi-Tsung Chen and Yau-Hwang Kuo, 2007. "Energy-Efficient Geographic Relay for Ad-Hoc Wireless Networks", 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp: 26-28.
10. Razia Haider, Muhammad Younas Javed and Naveed S. Khattak, 2007. "EAGR: Energy Aware Greedy Routing in Sensor Networks", Conf. on Future generation communication and networking.
11. B-Ghazaleh, N., K.D. Kang and K. Liu, 2005. "Towards Resilient Geographic Routing in Wireless Sensor Networks", 1st ACM Workshop on QoS and Security for Wireless and Mobile Networks, Montreal, Canada.
12. Marias, G.F., V. Tsetsos, O. Sekkas and P. Georgiadis, 2005. "Performance evaluation of a self-evolving trust building framework", Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks.
13. Karp, B. and H.T. Kung, 2000. "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", Mobi Com.
14. Zahariadis, T.H. P. Trakadas and H. Leligou, *et.al.*, 0000. "Securing wireless sensor networks towards a trusted Internet of Things", IoS Press, ISBN 978-1-60750-007-0, pp: 47-56.