Survey : Energy-Efficient and Trust-Aware Routing Techniques for WSN

Ms. Dipali Dikondwar
Dept of Computer Science and Engineering,
RCERT, Chandrapur (India)

Prof. R. K. Krishna
Dept of Electronics and Telecom Engineering
RCERT, Chandrapur.(India)

Abstract

Wireless Sensor Networks are gaining popularity due to the fact that they offer low-cost solutions for a variety of application areas, but efficient defense against security attacks is a challenging task in the wireless sensor network environment. Although significant research effort has been spend on the design of trust models to detect malicious nodes based on direct and indirect evidence, this comes at the cost of additional energy consumption. However, these networks are highly susceptible to attacks, due to both the open and distributed nature of the network, as well as the limited resources of the nodes, which dictate the implementation of sophisticated security frameworks. Some more techniques and algorithms than previous surveys, proposed on addressing these challenges are studied in this paper.

Keywords: WSN, trust-aware routing, energy efficient routing, secure routing, routing in WSN survey.

1. Introduction

Wireless Sensor Networks (WSN) are invading our everyday life with their proliferating applications which cover environmental observation, homeland security, building and factory monitoring and personal healthcare [2]. The small dimensions of sensor nodes combined with their low cost, further contribute towards wider penetration leading to exponentially increase of the number of deployed sensor nodes in the near future [2]. Due to recent technological advances, the manufacturing of small and low-cost sensors has become technically and economically feasible. These sensors measure ambient conditions in the environment surrounding them and then transform these measurements into signals that can be processed to reveal some characteristics about phenomena located in the area around these sensors. A large number of these sensors can be networked in many applications that require unattended operations, hence producing a wireless sensor network (WSN). Even from their earliest deployments, sensor networks have been attacked by adversaries interested in intercepting the data being sent or reducing the ability of the network to carry out its tasks. As the applications of WSNs become more complex and widespread, the ability to protect such systems has become increasingly important. Although military applications seem to have the strictest security requirements, issues like data confidentiality, data integrity and network availability are also important to any WSN application [2].

Typically, WSNs contain hundreds or thousands of these sensor nodes, and these sensors have the ability to communicate either among each other or directly to an external base station (BS). A greater number of sensors allows for sensing over larger geographical regions with greater accuracy.

Fig. 1 shows a schematic diagram of sensor node components. Basically, each sensor node comprises sensing, processing, transmission, mobilizer, position finding system, and power units (some of these components are optional, like the mobilizer). The same figure shows the communication architecture of a WSN. Each of these scattered sensor nodes has the capability to collect and route data either to other

IJERT

sensors or back to an external BS(s). A BS may be a fixed or mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data.

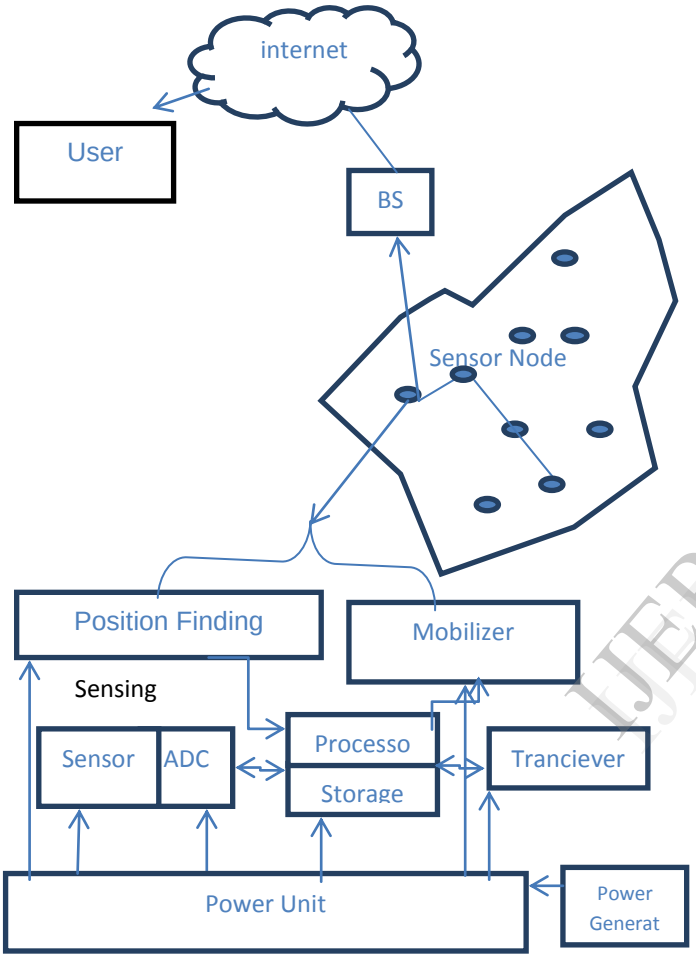

Fig 1.Components of Sensor Node
(Source: J. N. AL KARAKI, A. E. KAMAL, IEEE Wireless Communications, December 24, vol. 11., issue 6, pp. 28)

In the past few years, intensive research that addresses the potential of collaboration among sensors in data gathering and processing, and coordination and management of the sensing activity was conducted. In most applications, sensor nodes are constrained in energy supply and communication bandwidth. Thus, innovative techniques to eliminate energy inefficiencies that shorten the lifetime of the network and efficient use of the limited bandwidth are highly required. Such constraints combined with a typical deployment of large number of sensor nodes pose many challenges to the design and management of WSNs and necessitate energy-awareness at all layers of the networking protocol stack.

The rest of the paper is organized as follows- In section 2 we state challenges and design issues for energy efficient routing protocols in WSNs. Section 3 discusses some routing algorithms. Finally Section 4 concludes the paper and in 5 there are references.

2. Challenges and Design Issues

The design of energy-efficient routing protocols in WSNs is influenced by many factors. These factors must get over before efficient communication can be achieved in WSNs.

Here is a list of the most common factors affecting the routing protocols design:

- **Node Deployment:** It is an application-dependent operation affecting the routing protocol performance, and can be either deterministic or randomized.
- **Node/Link Heterogeneity:** The existence of heterogeneous set of sensors gives rise to many technical problems related to data routing and they have to be overcome.
- **Data Reporting Model:** Data sensing, measurement and reporting in WSNs depend on the application and the time criticality of the data reporting. Data reporting can be categorized as either time-driven (continuous), event driven, query-driven, or hybrid.
- **Energy Consumption Without Losing Accuracy:** In this case, energy-conserving mechanisms of data communication and processing are more than necessary.
- **Scalability:** WSNs routing protocols should be scalable enough to respond to events, e.g. huge increase of sensor nodes, in the environment.
- **Network Dynamics:** Mobility of sensor nodes is necessary in many applications; despite the fact that most of the network architectures assume that sensor nodes are stationary.
- **Fault Tolerance:** The overall task of the sensor network should not be affected by the failure of sensor nodes.
- **Connectivity:** The sensor nodes connectivity depends on the random distribution of nodes.
- **Transmission Media:** In a multi-hop WSN, communicating nodes are linked by a wireless medium. One approach of MAC design for sensor networks is to use TDMA based protocols that conserve more energy compared to contention-based protocols like CSMA (e.g., IEEE 802.11).
- **Coverage:** In WSNs, a given sensor's view of the environment is limited both in range and in accuracy;

IJERT

it can only cover a limited physical area of the environment.

- **Quality of Service:** Data should be delivered within a certain period of time. However, in a good number of applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than the quality of data sent. Hence, energy aware routing protocols are required to capture this requirement.
- **Data Aggregation:** Data aggregation is the combination of data from different sources according to a certain aggregation function, e.g. duplicate suppression.

All the above factors are discussed in detail in [1]. Routing in WSNs is very challenging due to the inherent characteristics that distinguish these networks from other wireless networks like mobile ad hoc networks or cellular networks. Following are the challenges and design issues for implementing routing protocols in WSN than other type of networks.

2.1 Large No of Sensor Nodes

Due to the relatively large number of sensor nodes, it is not possible to build a global addressing scheme for the deployment of a large number of sensor nodes as the overhead of ID maintenance is high. Thus, traditional IP-based protocols may not be applied to WSNs. Furthermore, sensor nodes that are deployed in an ad hoc manner need to be self-organizing as the ad hoc deployment of these nodes requires the system to form connections and cope with the resultant nodal distribution, especially as the operation of sensor networks is unattended. In WSNs, sometimes getting the data is more important than knowing the IDs of which nodes sent the data.

2.2 Flow of Sensed Data

In contrast to typical communication networks, almost all applications of sensor networks require the flow of sensed data from multiple sources to a particular BS. This, however, does not prevent the flow of data to be in other forms (e.g., multicast or peer to peer).

2.3 Energy Constraints

Sensor nodes are tightly constrained in terms of energy, processing, and storage capacities. Thus, they require careful resource management.

2.4 Stationary Nodes

In most application scenarios, nodes in WSNs are generally stationary after deployment except for maybe a few mobile nodes. Nodes in other traditional wireless networks are free to move, which results in unpredictable and frequent topological changes. However, in some applications, some sensor nodes may be allowed to move and change their location (although with very low mobility).

2.5 Application Specific N/W

Sensor networks are application-specific (i.e., design requirements of a sensor network change with application). For example, the challenging problem of low-latency precision tactical surveillance is different from that of a periodic weather monitoring task. Sixth, position awareness of sensor nodes is important since data collection is normally based on the location. Currently, it is not feasible to use Global Positioning System (GPS) hardware for this purpose. Methods based on triangulation.

2.6 Attacks

Security in WSNs means protection of information and resources from attacks and misbehaviors, while maintaining an acceptable level of operation even in the case of adverse conditions. The network layer attacks threatening the routing procedure form a long list as shown in Table I.

The description of each kind of attack is given in [4]. Also the countermeasures and limitations are discussed in [4].

Table 1: Network Layer Attacks & Behavior

Attack type	Attacker behavior
Selfish behavior (black-hole, greyhole)	A malicious node denies to perform benign routing and drops part or all the received packets.
Sinkhole attack	A malicious node tries to attract traffic advertising fake routing information, and then it refuses to forward it.
Replay attack	The original routing messages are repeated at a later time, thus deceiving the routing functionality.
Link Spoofing Attack	An adversary can spoof link layer acknowledgement for overheard packets to convince the sender that the

IJERT

	packet has been forwarded successfully.
Modification attack	An adversary modifies the data and/or routing packets it forwards.
Sybil attack	An attacker presents multiple identities.
Colluding nodes attack	Many powerful attackers work in collusion to modify or drop routing packets.
Traffic analysis	A malicious node monitors the traffic flows in order to identify, locate and attack the critical nodes (typically the base station).
Flooding attack	The attacker overwhelms a victim's limited resources, (e.g. memory) flooding the network with packets, which could be either data or routing packets.
On-off Attack	Malicious entities behave well and badly alternatively, hoping that they can remain undetected while causing damage.
Conflicting Behavior Attack	An attacker behaves inconsistently in the user domain and impairs good nodes' recommendation trust by performing differently to different peers.
Bad mouthing Attack	As long as indirect trust information is taken into consideration, malicious parties provide dishonest recommendations to frame up good parties and/or boost trust values of malicious peers.

Table 1 Source: T. Zaharadis, H. Leligou, P. Karkazis, P. Trakadas, IEEE Computer Society, 2010, pp 194-198.

2.7 Faulty/ Fraudulent Nodes

Some nodes in WSN may drop the data or send incorrect data. It is needful to detect such nodes to reduce data loss. Some approaches are also defined to calculate trust level of the nodes.

3. Routing Algorithms in WSNs

Due to such challenges, many new algorithms have been proposed for the routing problem in WSNs. These routing mechanisms have taken into consideration the inherent features of WSNs along with the application and architecture requirements [3]. The task of finding and maintaining routes in WSNs is nontrivial since energy restrictions and sudden changes in node status (e.g., failure) cause frequent and unpredictable To minimize energy consumption, routing techniques proposed in the literature for WSNs employ some well-known routing tactics as well as tactics special to WSNs, such as data aggregation and in network processing, clustering, different node role assignment, and data-centric methods.

Almost all of the routing protocols can be classified according to the *network structure* as flat, hierarchical, or location-based. Furthermore, these protocols can be classified into multipath-based, query-based, negotiation-based, quality of service (QoS)- based, and coherent-based depending on the *protocol operation* [1]. In flat networks all nodes play the same role, while hierarchical protocols aim to cluster the nodes so that cluster heads can do some aggregation and reduction of data in order to save energy. Location-based protocols utilize position information to relay the data to the desired regions rather than the whole network. The last category includes routing approaches based on protocol operation, which vary according to the approach used in the protocol.

In this article we explore some of these routing techniques in WSNs that have been developed in recent years.

3.1 TARP

L. Abusalah, A. Khokhar, G. BenBrahim, W. ElHajj in [9] proposed a Trust-Aware Routing Protocol (TARP) for secure-trusted routing in mobile ad hoc networks. In TARP, security is inherently built into the routing protocol where each node evaluates the trust level of its neighbors based on a set of attributes and determines the route based on these attributes. TARP selects routes to the destination based not only on the shortest path but also on several other security oriented attributes of the nodes. Only nodes that match the sender requirements would forward the packet. In TARP, the security parameters considered in computing the trust-level of a node in a given route include: *software configuration*, *hardware configuration*, *battery power*, *credit history*, *exposure* and *organizational hierarchy*.

IJERT

3.2 EAP

Ming Liu et al [7] propose a novel a distributed energy- aware routing protocol (EAP) for a long lived sensor network. In EAP, a node with a high ratio of residual energy to the average residual energy of all the neighbor nodes in its cluster range will have a large probability to become the cluster head. This can better handle heterogeneous energy circumstances than existing clustering algorithms which elect the cluster head only based on a node's own residual energy. After the cluster formation phase, EAP constructs a spanning tree over the set of cluster heads. Only the root node of this tree can communicate with the sink node by single-hop communication. Because communications in in-network can be computed by the free space model, the energy will be extremely saved and thus leading to sensor network longevity.

3.3 ATSR

In [6], Theodore Zahariadis et al have given a secure routing protocol (Ambient Trust Sensor Routing, ATSR) which adopts the geographical routing principle to cope with the network dimensions and relies on a distributed trust model for the detection of malicious nodes. Both direct and indirect trust information is taken into account to evaluate the trustworthiness of each neighbour. An important feature is that it takes into account the remaining energy of each neighbour, thus allowing for better load balancing and network lifetime extension. As soon as the malicious nodes are detected, the network performance becomes identical to the one observed for no malicious nodes in the network. ATSR bases its decisions on local information which renders it suitable for large wireless sensor networks while at the same time, node and network resources are economized.

3.4 TARF

Guoxing Zhan et al [5] presented TARF, a trust aware routing framework for WSNs. TARF secures the multi-hop routing in WSNs against intruders exploiting the replay of routing information by evaluating the trustworthiness of neighboring nodes. It identifies such intruders that misdirect noticeable network traffic by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory *throughput*. It is also energy-efficient with acceptable overhead, highly scalable, and well adaptable. It incorporates the trustworthiness of nodes into routing decisions and allows a node to circumvent an adversary misdirecting considerable traffic with a forged identity attained through replaying.

3.5 TER

Laura Gheorghe et al [8] developed TER - Trust and Energy-aware Routing protocol, a location-based, trust and energy-aware, routing protocol for Wireless Sensor Networks. The protocol uses distance, trust and energy as metrics when choosing the best path towards the destination. TER uses trust values, energy levels and location information in order to determine the best paths towards a destination. The protocol achieves balancing of traffic load and energy, and generates trustworthy paths when taking into consideration all proposed metrics.

4. Conclusions

In this paper we studied challenges and design issues in implementing energy efficient routing protocols in wireless sensor networks, various kinds of attacks and its behavior. And lastly different algorithms that take into consideration the energy, trust and distance matrices of the sensor network nodes. In future we can implement and do comparative study of these energy and trust aware algorithms.

5. References

[1] J. N. Al-Karaki, A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Wireless Communication, December 2004, pp 6-28.
[2] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, "Energy efficiency and implementation cost of trust aware routing solutions in WSNs", IEEE Computer Society, 14th Panhellenic Conference on Informatics 2010, pp 194-198.
[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, August 2002, pp 102-114.
[4] C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", First IEEE Workshop on Sensor Network Protocols and Applications 2003.
[5]G. Zhan, W. Shi, and J. Deng, "TARF: A trust aware routing framework for wireless sensor networks", in proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10) 2010.
[6] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, S. Voliotis, S. Maniatis, " An Energy and

IJERT

Trust aware routing Protocol for Large WSNs", proceedings of the 9th WSEAS Intenational Conference on Applied Informatics and Communiacations, 2009, pp 216-224.

[7] M. Liu, J. Cao, G. Chen, and X. Wang, "An energy aware routing protocol in wireless sensor networks", Sensors 2009, pp. 445-462.

[8]L. Gheorghe, R. Rughinis, M. Tapus, "Trust and energy aware routing protocol for wireless sensor networks", ICWMC 2012, pp. 388-394.

[9]L. Abusalah, A. Khokhar, G. BenBrahim, W. ElHajj,"TARP: Trust-Aware Routing Protocol",IWCMC'06, July 3-6 2006, pp. 135-140.

IJERT