SCARP: Secure Congestion Aware Routing Protocol for Wireless Sensor Networks

Ch.Radhika Rani, S.Nagendram, Subba Reddy Oota
Department of Computer Science
Koneru Lakshmaiah College of Engineering
Vijayawada, India
radhijaya@gmail.com, reena1286@gmail.com, subbareddy4ever@gmail.com

***Abstract*— Wireless sensor networks sense various kinds of information, process them locally and communicate it to the outside world via satellite or Internet. In the near future, sensor networks will play a major role in collecting and disseminating information from the fields where ordinary networks are unreachable for various environmental and strategical reasons. Hence it is increasingly likely that sensors will be shared by multiple applications and gather heterogeneous data of different priorities. With such concentration on wireless sensor networks, vital issues like security and congestion control are to be taken care of. We propose Secure Congestion Aware Routing protocol (SCARP), a protocol designed for mitigating congestion by dedicating a portion of network to forward high-priority traffic primarily and also satisfies the major security properties like data authentication, data secrecy, replay protection, freshness with low energy consumption which are the major factors affecting the wireless sensor networks.**

Keywords-Wireless sensor networks; Routing; Congestion control; Data security; Energy efficiency

I. INTRODUCTION

Wireless sensor networks are being used in various areas of life, hence deploying such large-scale networks has a high cost, it is increasingly likely that sensors will be shared by multiple applications like environment monitoring, health monitoring, military sensing and tracking, etc. There can be various types of data transmitted by sensor network such as temperature, the presence of lethal chemical gases, audio and/or video feeds, etc. Therefore, data generated in a sensor network may not all be equally important. Thus the case of priority occurs dividing data into high and low priority. In hostile and untrusted environments such as battlefield surveillance, an adversary can eavesdrop on traffic, inject new messages, and replay old messages. Hence security is of major concern.

With the vast applications and usage of wireless senor networks, congestion becomes an important problem. Congestion may lead to indiscriminate dropping of data packets. It also results in an increased consumption of energy to route packets that may be dropped downstream as links become saturated. As nodes along optimal routes are depleted of energy, only non optimal routes remain, further compounding the problem. To ensure that data with higher priority is received in the presence of congestion due to LP (Low Priority) packets, differentiated service must be provided by diverting the LP packets in the routes other than the conzone path formed by the HP (High Priority) packets to mitigate the congestion.

Usage of wireless senor networks in various applications including vital areas where there is a chance of compromising the privacy of data, hence the transfer of data should be done in a secure manner. In order to add security, the various areas such as Authentication, Secrecy, Replay Protection, and Resilient to Lost Messages are to be taken care of. We use OCB (Offset Code Book) encryption scheme that covers all the areas addressed above. OCB scheme is well-suited for the stringent energy constraints of sensor nodes.

In this paper, we are interested in congestion that results from excessive competition for the wireless medium and security for the data that is transferred by the wireless networks. Existing solutions detect and solve congestion or provide security to data but not both as a whole. We propose SCARP, Secure Congestion Aware Routing Protocol that addresses congestion control by the categorization and distinct routing of data as high priority and low priority along with the secure communication of data handled by the use of OCB encryption scheme.

The main contributions of this paper are as follows.

- We introduce SCARP Secure Congestion Aware Routing Protocol that efficiently addresses the aspects of congestion control and security in wireless sensor networks.
- Congestion control is efficiently handled by prioritizing the data in the network.
- High-level security is provided via authentication, secrecy and replay protection.

- We measure the performance of SCARP and show that, under various scenarios, SCARP is efficient and effective.
- We combine the security and congestion control, which are the prime areas of concern in wireless senor networks.
- The protocol is energy efficient as there is low energy overhead.

II. RELATED WORK

An obvious solution to enhance service to HP data is to use priority queues to provide differentiated services ([1], [2], and [3]). However, in such schemes, though HP packets get precedence over LP packets within a node, at the MAC layer, they still compete for a shared channel with LP traffic sent by surrounding nodes. As a result, without a routing scheme to address the impact of congestion and hotspots in the network, local solutions like priority queuing are not sufficient to provide adequate priority service to important data. QoS in sensor networks has been the focus of current research ([1], [4], and [5]).

Degrading service to one type of data to provide better service to another has been used in schemes like RAP [2] and SWAN [6]. Many of the schemes do not adopt differentiated routing, which leverages the large uncongested parts of the network that is often underutilized to deliver LP traffic. Hence we use differentiated routing to provide the best possible service to HP data while trying to decrease the energy consumption in the conzone.

Congestion in sensor networks has been addressed in works like CODA [7] and Fusion [8]. Though these schemes take important steps to mitigate congestion in sensor networks, they treat all data equally. Priority based schemes have been addressed in CAR and MCAR [9].

Several encryption modes exist that achieve secrecy and authentication. We select OCB [10] as our encryption mode since it is especially well-suited for the stringent energy constraints of sensor nodes. In addition to OCB, SCARP also uses loose time synchronization to minimize energy consumption and can be used to provide efficient replay protection in broadcast communication similar to Minisec[11]. In this section, we briefly review OCB.

OCB, or Offset Code Book, is a block-cipher mode of operation that features authenticated encryption. Given a plain text of arbitrary length, OCB generates a cipher text that simultaneously provides authenticity and data secrecy. OCB is provably secure, and is parameterized on a block cipher of block size *n* and a tag of length t. t is defined such that an adversary is able to forge a valid cipher text with probability of 2^{-t} . OCB operates as follows.

OCB is especially well suited for sensor nodes. OCB avoids cipher text expansion. OCB has superior performance, since it provides secrecy and authenticity in one pass of the block cipher. TinySec and ZigBee provide the same security guarantees, but require two passes of the block cipher: one pass achieves secrecy with CBC-encryption, and another pass achieves authenticity with CBC-MAC. Consequently, since TinySec almost doubles the amount of computation, the energy consumption also doubles. OCB requires very few block cipher calls when compared to CBC-encryption and CBC-MAC schemes.

III. SCARP: SECURE CONGESTION AWARE ROUTING PROTOCOL

We present SCARP, a secure congestion aware routing protocol that discovers the congested zone of the network that exists between high-priority data sources and the data sink. Using simple forwarding rules, this portion of the network is dedicated to forward high-priority traffic primarily. It also satisfies all the security properties like data authentication, data secrecy, replay protection, freshness with low energy consumption which are the major factors affecting the Wireless Sensor Networks.

A. Overview

An important event occurs in one portion of the sensor field called the critical area. This critical area will typically consist of multiple nodes. In such a scenario, there is a data processing center for collecting sensitive information from the critical area called sink. We refer to the area that contains the shortest paths from the critical area to the sink as the conzone. Our basic solution, called SCARP, operates solely in the network layer. Packets are classified as HP or LP by the data sources, and nodes within a conzone only forward HP traffic. LP traffic is routed out of and/or around the conzone. Also, the sources employ OCB-encryption to encrypt the data before communicating the data in order to provide security. The sink, upon receiving the packet decrypts the data.

B. Description

In this section, we describe the mechanisms of SCARP in the network scenario where there are multiple sources and a single high priority sink.

SCARP comprises of the following five steps:

1) Formation of High-Priority Routing Network

After the deployment of sensor nodes, Sink initiates the process of building the HP routing network (HiNet). This network covers all nodes, because at the time of deployment, the sink will usually have no information on the whereabouts of the critical area nodes. Since all HP data is destined to a single sink, the HiNet is based on a

minimum distance spanning tree rooted at the sink. A node that has multiple neighbors with depths (the number of hops to the sink) less than its own considers them all as parents.

We now consider the HiNet formation process. Once the sink discovers its neighbors, it broadcasts a "Build HiNet" message (containing the ID and depth of the node) asking all nodes in the network to organize as a graph. Once a neighboring node hears this message, it checks if it has already joined the HiNet (i.e., if it knows its depth); if not, it sets its depth to one plus the depth in the message received and sets the source of the message as a parent. Similarly this node then rebroadcasts the Build HiNet message, with its own ID and depth. If a node is already a member of the graph, it checks the depth in the message, and if that depth is one less than its own, then the source of the message is added as a parent. In this case, the message is not rebroadcast. Finally, the Build HiNet message is rebroadcast with the new depth value. In this fashion, the Build HiNet message is sent down the network until all nodes become part of the graph.

2) Conzone Discovery

Nodes discover if they are on the conzone by using the conzone discovery mechanism. This conzone discovery is done dynamically, because the critical area can change during the lifetime of the deployment and is triggered when an area starts generating HP data. A conzone must be then discovered from that neighborhood to the sink for the delivery of HP data. To do this, critical area nodes broadcast "discover conzone to sink" (ToSink) messages. This message includes the ID of the source and its depth and is overheard by all neighbors. When a node hears more than α_x (neighborhood size) distinct ToSink messages coming from its children, it marks itself as on conzone and propagates a single ToSink message. For node x with depth d_x and neighborhood size n_x, setting correctly for different depths ensures that the conzone is of an appropriate width.

ToSink Threshold : $\alpha_x = \beta_{d_x} . d_x . n_x$

An important goal of the conzone discovery algorithm isto split the parents and siblings (nodes with the same depth) in the HiNet into on-conzone and off-conzone neighbors. Since the presence of a conzone leads to suboptimal routing for LP data due to on-conzone nodes being dedicated to serving HP data, after the HP stream comes to an end, the conzone is destroyed by flooding a "destroy conzone" message in the conzone.

3) Encryption

We assume that symmetric keys K_{A_iB} , $K_{BA_i}$are already established between each source A_i and the sink B. We recommend a different key for each source, but our protocol is by no means restricted to such a setup. A monotonically increasing counter is assigned to each key as the Initialization Vector IV (C_{A_iB}used to for key K_{A_iB}), and is kept as internal state by both sender and receiver.

We employ OCB-encryption with the packet payload as M, packet header as H, counter C_{A_iB} as the nonce, and K_{A_iB} as the encryption key. We selected Skipjack to be the underlying block cipher with a block size of 64 bits. Since OCB requires the nonce to be the same length as the block size, counter C_{A_iB} can also be 64 bits. Alternatively, the counter could be of shorter length, and be padded out to 64-bits when requested by the OCB encryption function. The second parameter of OCB is the tag length τ, which we set to 32 bits, a length suitable for security in retail banking [10]. Sink B maintains a buffer of counters C_{A_1B}, C_{A_2B}... C_{A_iB} for all the sources A_1, A_2,...A_n. The source increments its counter value by one before sending each message.

4) Differentiated Routing

After the message is encrypted, HP data is routed in the conzone and LP data is routed off the conzone. LP data generated inside the conzone is routed out using the following approach. When an on-conzone node gets an LP message, it forwards it to an off-conzone parent, if there are any. Otherwise, the LP data is forwarded to an off-conzone sibling. If there are no parents or siblings that are off conzone, we resort to the following method. After discovering the conzone, the sink sends a message through the conzone, which contains the coordinates of a line that cuts the conzone in half. This line connects the sink to the center of the critical area. Using this information and its own coordinates, a node can determine on which half of the conzone it lies and hence routes LP data to the parent that is closest to the conzone boundary, i.e., farthest from the line. With the assumption of uniform deployment density, this ensures that all LP data generated inside the conzone is routed out efficiently and along the shortest path.

We used AODV in the off-conzone nodes to route LP data, with the modification that the on-conzone nodes do not propagate route request or reply messages for LP data. Using this modified routing scheme, LP data generated outside or routed out of the conzone is routed to its destination via off-conzone nodes only.

5) Decryption

Upon receiving the message, sink B decrypts it with the key K_{BA_i} of the corresponding sender A_i. Sink then increments its local copy of C_{A_iB} accordingly so that it remains consistent with A_i.

C. Security analysis

In this section, we provide an analysis on the level of security promised by SCARP.

1) Authentication: SCARP uses OCB encryption to provide data authentication over the payload and packet header. The security of OCB's authentication scheme is directly related to . , the length of the tag. By setting . to be 32 bits, an adversary has a 1 in 2^{32} chance of forging a correct tag for a particular message. This suffices for the majority of practical applications.

2) Secrecy: Semantic security requires that nonces do not repeat. In SCARP, the counter is kept as internal state, and thus can be made arbitrarily long. We choose 8 bytes, which means that the nonce would not repeat until after sending 2^{64} messages.

3) Replay protection: Each sender and receiver keeps a synchronized counter that is used as the nonce in OCB encryption.The receiver would only accept messages with higher counter values than the those maintained in the node state. Thus, replayed packets will all be rejected.

4) Freshness: In SCARP, the receiver can arrive at the counter value used for each packet by verifying the validity of OCB decryption. The receiver can use the counter value of two messages to enforce message ordering, thus providing freshness.

IV. ALGORITHM

Local Variables

Off-conzone parents: $P_{off} = \{p_1, p_2, \ldots\ldots, p_n\}$
Off-conzone siblings: $S_{off} = \{s_1, s_2, \ldots\ldots, s_n\}$
On-conzone parents: $P_{on} = \{\}$
On-conzone siblings: $S_{on} = \{\}$
Children: Children = $\{c_1, c_2, \ldots\ldots, c_k\}$
Node's on-conzone status: On_conzone = FALSE
ToSink message received: ToSink_received = 0
ToSink threshold: $\alpha_x = \beta_{d_x} . d_x . n_x$

Conzone Discovery :

if node x receives ToSink from child c_1 **then**
  if On_conzone == FALSE **then**
    if ToSink_received > α_x **then**
      On_Conzone = TRUE
      if x is not sink then
        broadcast ToSink with d_x
      else
        ToSink_received ++
else if node x receives ToSink from parent p_j **then**
  P_{off} - = $\{p_j\}$; P_{on} + = $\{p_j\}$
else if node x receives ToSink from sibling s_i **then**
  S_{off} - = $\{s_i\}$; S_{on} + = $\{s_i\}$

Encryption:

//Encrypt the payload M with the symmetric key K_{A_iB}
Encrypt(M, K_{A_iB})
Counter C_{A_iB} ++
Assign the counter as nonce to key as IV
if length of C_{A_iB} < 64 bits **then**
  Pad the counter with zeros
//Set tag length τ
τ = 32 bits

Differentiated Routing:

if $P_{on} \neq \{\}$ **then**
  Send data to any p ϵ P_{on}
else if ∃ a sibling s ϵ S_{on} then
  send data to s
else
  send data to any u ϵ P_{off} U S_{off}

Decryption:

//Decrypt the message with the key K_{BAi}
Decrypt(M, K_{BA_i})
Identify the counter of the source A_i
//Increment the local copy of C_{A_iB}
Counter C_{A_iB}++

V. EXPERIMENTAL RESULTS

The simulations were conducted in NS-2 [12], with a deployment area of 560m X 360m. In this area, 150 nodes were placed in a 15x10 grid with the separation between neighboring nodes along both axes being 40 m.

In this group of simulations, the transmission ranges were varied between 90, 130, 170, and 210 m. As the transmission range increases, the number of hops from the edge of the network to the sink decreases from 6 to 3. The LP data rate of each node, other than the critical area nodes and the sinks, was set to 0.5 pps, while the HP data rate of critical area nodes was set to 30 pps. These simulations show the gains of SCARP.

A. Reliablilty

Figure 1 plots the fraction of HP data delivered to the sink. As the transmission range increases, the network becomes more congested, and more collisions occur. As a result, the performance of AODV degrades severely, and it routes less than 10 percent of HP data successfully. On the other hand, AODV+PQ and SCARP route a higher fraction of the data, SCARP routes more HP data than AODV+PQ for all ranges proving the reliability of protocol.

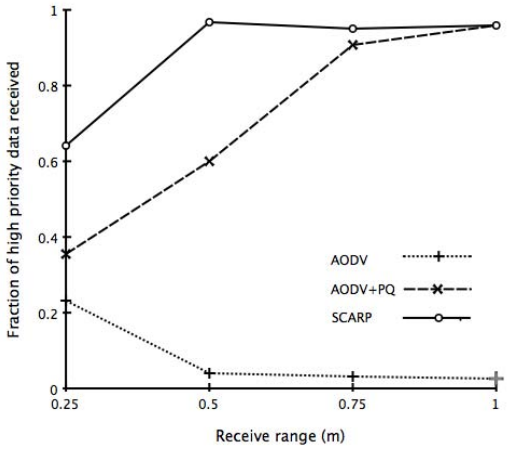

Figure 1. HP data delivery fraction

Figure 2 shows the fraction of LP data routed successfully. Although our focus is to provide better service to HP data in the presence of congestion, SCARP also effectively utilizes the uncongested off-conzone nodes to prevent severe degradation of LP data. SCARP routes more LP data than AODV as the range increases. AODV+PQ routes more LP data than SCARP, because it does not as aggressively degrade service to LP data as SCARP. Hence reliabilty is provided for LP packets too.

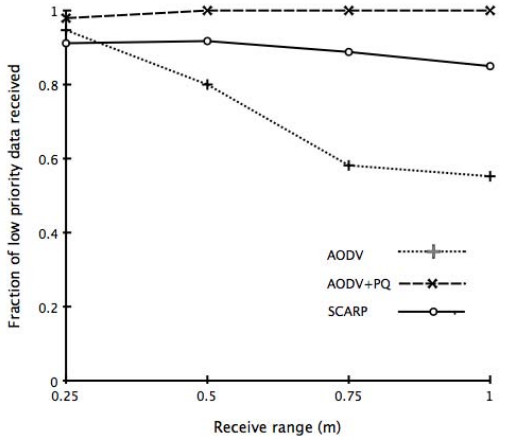

Figure 2. LP data delivery fraction.

B. Delay

Figure 3 shows that as the range increases, the average HP data delivery delay for AODV increases while such delay for AODV+PQ and SCARP decreases. This is due to the increasing congestion that AODV faces. Furthermore, the jitter introduced by data forwarding is always less for SCARP as compared to AODV and AODV+PQ.

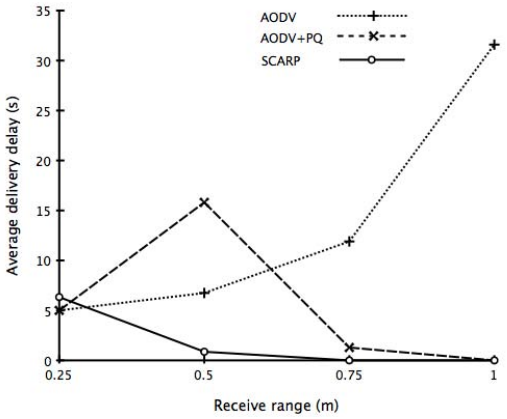

Figure 3. HP data delivery delay for various protocols.

C. Energy Consumption

The maximum energy used by any node in the deployment is depicted in Figure 4. This includes the energy used to route all possible traffic, both LP and HP. The energy used by AODV and AODV+PQ is more than that for SCARP.

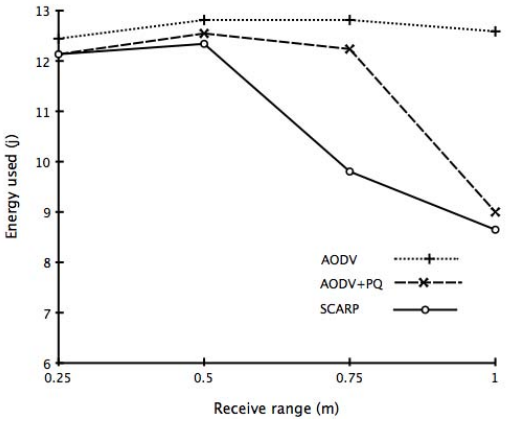

Figure 4. Maximum node energy used for various transmission ranges

VI. CONCLUSION

In this paper, we addressed data delivery issues in the presence of congestion in wireless sensor networks. We proposed SCARP, which is a secure differentiated routing protocol and uses data prioritization. Our extensive simulations show that as compared to AODV and AODV+PQ, SCARP increases the fraction of HP data delivery and decrease delay and jitter for such delivery while using energy more uniformly in the deployment. SCARP also routes an appreciable amount of LP data in the presence of congestion. Our secure sensor network communication protocol, SCARP, offers a high level of security while requiring much less energy than previous approaches.

REFERENCES

[1] K. Akkaya and M.F. Younis, ,ÄúAn Energy-Aware QoS Routing Protocol for Wireless Sensor Networks,,Äù Proc. 23rd IEEE Int,Äôl Conf. Distributed Computing Systems (ICDCS ,Äô03), pp. 710-715, 2003.

[2] C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He, ,ÄúRAP: A Real-Time Communication Architecture for Large-Scale Wireless Sensor Networks,,Äù Proc. Eighth IEEE Real-Time and Embedded Technology and Applications Symp. (RTAS ,Äô02), pp. 55-66, 2002.

[3] H. Zhang, A. Arora, Y. Choi, and M. Gouda, ,ÄúReliable Bursty Convergecast in Wireless Sensor Networks,,Äù Proc. ACM MobiHoc, 2005.

[4] T. He, J.A. Stankovic, C. Lu, and T. Abdelzaher, ,ÄúSpeed: A Stateless Protocol for Real-Time Communication in Sensor Networks,,Äù Proc. 23rd IEEE Int,Äôl Conf. Distributed Computing Systems (ICDCS), 2003.

[5] Y. Zhang, M.P.J. Fromherz, and L.D. Kuhn, ,ÄúSmart Routing with Learning-Based QoS-Aware Meta-Strategies,,Äù Proc. First Workshop Quality of Service Routing (WQoSR ,Äô04), pp. 298-307, 2004.

[6] G.-S. Ahn, L.-H. Sun, A. Veres, and A.T. Campbell, ,ÄúSwan: Service Differentiation in Stateless Wireless Ad Hoc Networks,,Äù Proc. IEEE INFOCOM, 2002.

[7] C.-Y. Wan, S.B. Eisenman, and A.T. Campbell, ,ÄúCODA: Congestion Detection and Avoidance in Sensor Networks,,Äù Proc. First ACM Conf. Embedded Networked Sensor Systems (SenSys ,Äô03), pp. 266-279, 2003.

[8] B. Hull, K. Jamieson, and H. Balakrishnan, ,ÄúMitigating Congestion in Wireless Sensor Networks,,Äù Proc. Second ACM Conf. Embedded Networked Sensor Systems (SenSys), 2004.
[9] Luk, M. Mezzour, G. Perrig, A. Gligor, V., 6th International Symposium on Information Processing in Sensor Networks, 2007.
[10] P. Rogaway, M. Bellare, and J. Black. OCB: A block-cipher mode of operation for efficient authenticated encryption. In ACM TISSEC, November 2001.
[11] Kumar, R. Crepaldi, R. Rowaihy, H. Harris, A.F. Guohong Cao Zorzi, M. La Porta, T.F,"Mitigating Performance Degradation in Congested Sensor Networks",IEEE Transactions on Mobile Computing,2008.
[12] ns2: Network Simulator, http://www.isi.edu/nsnam/ns/, 2008.