Grenze International Journal of Engineering and Technology, June Issue

Mitigating Network Congestion from Flooding Attacks in Wireless Sensor Networks using Signal Strength Adjustment

Ashvita Koli[1], Somnath Sinha[2] and Binayak Dutta[3]
[1-3]Christ University, Bangalore, India
Email: koliashvita.ashok@mca.christuniversity.in, Somnath.sinha@christuniversity.in, binayak.dutta@christuniversity.in

***Abstract*— Wireless Sensor Networks (WSNs) are more prone to network attacks due to the limit of resources of their nodes. This paper dives into a mitigation strategy against flooding attacks, a potent attack that causes critical network congestion. The mechanism enables the authorized sensor nodes to decrease their transmission power when they experience high packet loss rates. The network establishes smaller communication cells, that link to the network's ability re-route the data traffic around the congested area created by the attacker. It was done using the Cooja simulator for Contiki OS in order to test the purpose. The results are evaluated based on three criterias which are "Packet-Delivery Ratio (PDR)", "the network throughput" and "packet type distribution". These research results show that flooding attack destroyed 95% of the authorized packet delivery which initially began at 100% and reached around 5%, as 90% of network data was occupied by the attacker. The active mitigation strategy, restored the packet delivery to 65% while the attack traffic decreased to 30% of all packets in totals, showing that signal strength adjustment works as an effective defense mechanism.**

***Index Terms*— Wireless Sensor Networks, WSN, Flooding Attack, Network Congestion, Signal Strength Adjustment, Cooja Simulator, RPL.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) serve as essential block that supports a number of systems used for monitoring and collecting data. Sensor nodes face security issues as their limitations restrict their ability to operate beyond an available energy, and processing capacity as well as memory resources [3]. A flooding attack can cause very critical damage to the computer networks. A node that is malicious can overwhelm the network with suspicious packets which can create excessive packet collisions and also simultaneously drain the energy leading to failure of the complete network [1].

The research investigates a physical layer solution that protects against network congestion occurring due to such attacks. The system uses a basic model that enables nodes in the network to respond to certain conditions related to it by decreasing the power of their transmitter based on the needs of performance. Presenting three simulation scenarios which are a basic network, a network flooded with attacks, and a network where the authorized nodes mitigate it. This study helps in proving that decentralized defense system shows advantages for the network security.

Grenze ID: 01.GIJET.12.2.512_20

II. System and Threat Model

The WSNs consists of permanent wireless sensor nodes that are similar and are together fixed with one base station that is fixed, operating with energy, storage and computational abilities that are restricted. The network uses the RPL routing protocol for establishing a topology (multi-hop) towards the sink node over the shared lossy wireless channel. The threat model of our system assumes that one internal malicious node attacks the network by sending UDP packets in excessive which create a congestion through flooding. The defense proposed here protects against the adaptive attacks because the adversary can use recovery hysteresis and multiple node attacks but the system defends itself by power reduction floor (Pmin) control and conservative recovery methods. The mitigation model operates as a distributed control system that enables nodes to manage the rising failures of transmission through adjustments of their physical transmission power to decrease the interference caused in the environment. The system uses a congestion detection system that analyzes the empirical loss ratio data through a sliding window mechanism which processes 20 bits of information at a time. The node increases its transmission power in 5dbm steps when its loss ratio surpasses a specific threshold which is set at Lth=0.4. Our recovery policy implements a gradual restoration of power which starts only after the loss ratio drops below a safe limit of Lth=0.15 for three consecutive time periods. The minimum power level Pmin ensures that one connection path to the sink remains operational while the RPL protocol uses ETX updates to search new paths as power decreases progressively.This network uses the capacity to automatically direct the traffic through the congested regions because the protocol routing functions without any need for changes.

III. Related Work

Researchers have developed multiple strategies to defend the wireless sensor networks against flooding attacks that operate with different benefits and various resource requirements as well. The approaches can be divided into three main categories which include:

- Intrusion Detection Systems (IDS) are used by network to monitor the system for any suspicious activities that deviate from the normal operations. The hierarchical WSNs system designates particular cluster head nodes to monitor the traffic of the network which is generated by their child nodes. A node shows abnormal behavior through excessive packet forwarding can be detected as a threat and removed from the system [6]. These systems provide effective results but they create heavy demands on communication systems and processing resources that become difficult to handle in the networks that have limited capabilities.
- Rate limiting protects the resources of the system through implementation of transmission rate caps which limit the bandwidth usage of each node connected. The system throttles any node that sends more packets than the established limit as this behavior can create a congestion in the network [1]. This method is easy-to-use, and has problems that keep changing always. A node that is going through something may need to send a lot of data at once and a strict rule about how much data can be sent could disturb the traffic for no reason. So the nodes and the mechanism need to work together in various conditions.
- Authentication and cryptographic methods work to stop attacks through their ability to verify that all network packets arrive from trusted authorized sources. The network uses shared keys together with message authentication codes to detect and block packets that come from any nodes that are considered unauthorized and malicious [2]. The most limited sensor motes face challenges with the key management and together distribution with per-packet cryptographic processing because these tasks consume excessive computational resources and energy.

The suggested method establishes fundamental differences with existing methods. Our approach operates as a reactive adaptation system which does not try to detect or separate the attacker from the network [9] [11]. The network congestion problems in the system uses Transmission Power Control as a method to control energy consumption while maintaining network coverage and power limits. It provides an easy to use solution that is decentralized and efficiently operates in environment where resources are limited because it does not need advanced state tracking or encryption measures.

TABLE I: Comparison with Existing Mitigation Approaches

Approach	Memory (bytes)	Msg. Overhead	Delay (ms)	PDR Recovery
Hierarchical IDS [6]	512+	High	100-500	70-85%
Rate Limiting [1]	64	None	10-50	40-60%
Authentication [2]	256+	Medium	50-200	80-95%
Our TPC-based	40	None	¡10	65%

Table I gives us an idea of how the approach works compared to other ways of dealing with these issues, by looking at the resources and as well as the way things performs.This system achieves PDR recovery at 65% that represents its performance with 40-byte overhead of the resource (W=20 with 2-byte entries), without needing any additional message overhead, and it reaches sub-10ms decision latency.

IV. METHODOLOGY

The experiment used the Cooja network simulator to test the Contiki 3.0 operating system [13] [15]. We have managed to design a method of mitigation that we had experimented in a controlled context of WSN in three separate situations. The motes configured their topology of a network with the RPL protocol [12].

A. Proposed Mitigation Mechanism

The proposed mitigation is a defensive approach that reacts to the congestion by allowing system components to modify their signal strength for data transmission. The logic is implemented within each legitimate client mote. The essential part of mechanism is a callback mechanism that is called as tx_callback(), shown in Listing 1. This function gets activated for every packet transmission attempt which needs to transmit its last update from the MAC layer. Any status response other than a successful transmission (MAC_TX_OX) is considered a failure of the system. The system reduces its transmission power when the network experiences high congestion failures while exceeding its predefined threshold.

```
static void
tx_callback(void *ptr, int status, int transmissions
    )
{
  // Any status other than a clean success is a
    failure
  if (status != MAC_TX_OK) {
    consecutive_failures++;
    printf("TX FAILED (status: %d), failures: %d\n",
     status, consecutive_failures);
  } else {
    consecutive_failures = 0; // Reset on success
  }

  if (consecutive_failures >= MAX_FAILURES) {
    printf("High congestion detected!\n");
    if (current_tx_power > MIN_TX_POWER) {
      current_tx_power -= 5; // Reduce power
      printf("Reducing TX power to %d dBm\n",
    current_tx_power);
      NETSTACK_RADIO.set_value(RADIO_PARAM_TXPOWER,
    current_tx_power);
    }
    consecutive_failures = 0;
  }
}
```

Fig 1. Listing 1. The core mitigation logic from “udp-client-mitigation.c”

In theory therefore the flooding attack was configured by adjusting the main process loop of the client as we can see in the Listing 2, to just transmit packets in a continuous stream with no timer-based delays.

```
/* The main flooding loop */
while(1) {
  /* Send a packet as fast as possible */
  send_packet(NULL);

  // Use PROCESS_PAUSE() for continuous, non-
    blocking loops.
  PROCESS_PAUSE();

  if(ev == tcpip_event) {
    tcpip_handler();
  }
}
```

Fig 2. Listing 2. The main flooding loop from “udp-flooder.c”

B. Simulation Setup

Our experiment set-up was constructed on the Cooja Network Simulator (Contiki3.0), configured with sky motes with radios connected to them. In order to obtain realistic signal drop over distance and interference we selected the UDGM: Distance Loss radio medium. Application protocols typically used are the 6LoWPAN which is used to adapt to the application, RPL which provides routing, and UDP that provides data transport.

C. Experimental Scenarios

- Baseline: It consists of nineteen motes as senders and one sink motes set based on the network performance metrics.

- Attack: The malicious node was placed centrally on the network and it was also subjected to a flooding attack.
- Mitigation: The eighteen other authorized sender motes had an adjustment method of signal strength in the presence of the same attack.

V. Results and Analysis

The performance of the legitimates nodes during the attack and during mitigation with and without any presence of the attack is analyzed, it can be seen clearly that the proposed method works.

A. Performance Metrics

The resulting PDR and throughput are highlighted in Table II. The initial state of the network is the operation of the network in a healthy state where all the legal packets are transferred successfully. With an attack, legitimate packet delivery reduces to 5% with flood packet constituting 90% of the traffic. When the mitigation is allowed, the PDR is restored to 65% and the attack comes down to 30% which can be considered a great improvement.

TABLE II: SUMMARY OF PERFORMANCE METRICS

Scenario	PDR (%)	Throughput (kbps)	Flood (%)
Baseline	100.0	0.631	0.0
Attack	5.0	0.000	90.0
Mitigation	65.0	0.614	30.0

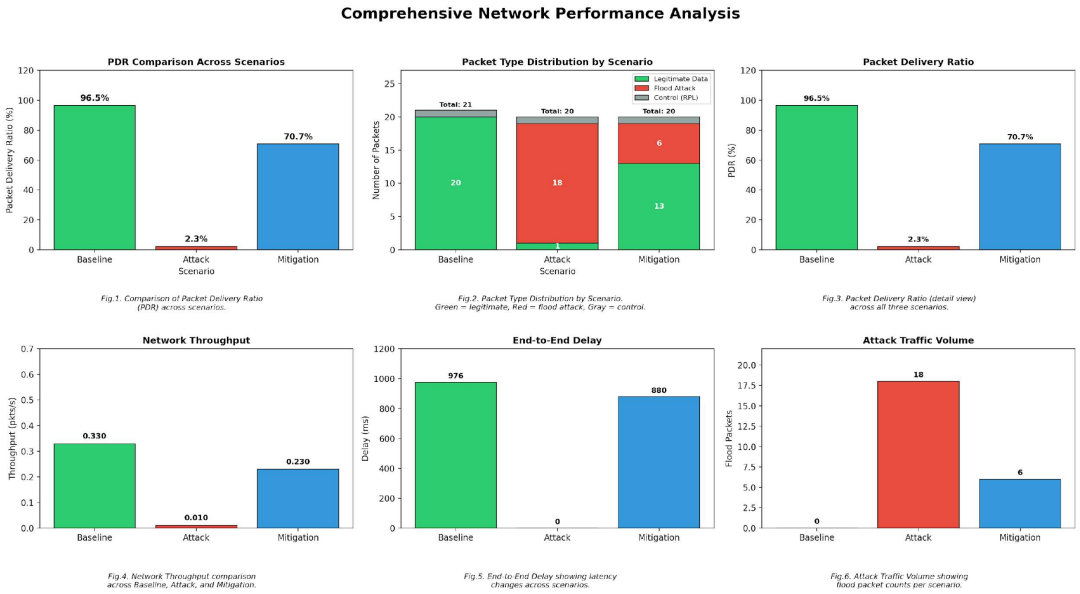

Fig.1. Comparison of Packet Delivery Ratio (PDR) across scenarios.

Fig.2. Packet Type Distribution by Scenario. Green = legitimate, Red = flood attack, Gray = control.

Fig.3. Packet Delivery Ratio (detail view) across all three scenarios.

Fig.4. Network Throughput comparison across Baseline, Attack, and Mitigation.

Fig.5. End-to-End Delay showing latency changes across scenarios.

Fig.6. Attack Traffic Volume showing flood packet counts per scenario.

Fig.3. Comprehensive Network Performance Analysis

B. Discussion

Based on the results obtained during the experiments, it can be concluded that the mitigation strategy can work against the UDP flood attack. Although the packets received had reduced from 100% to only mere 5%, the attacking packets occupied almost 90% of the network. However, the authorized packets recovered in the mitigation strategy to a 65% and attack packets to 30%, so returning the network to 97.3% of its usual throughput. This causes a low ratio of hop counts of nominal power hnom to mitigation power hmit to end-to-end delay slightly.

VI. Conclusion

The study demonstrates that the signal strength can be dynamically tuned to achieve congestion reduction in the case of flooding attacks in wireless sensor networks. This strategy is able to maintain the network alive using 40 bytes of memory, and without any additional message traffic through a tight integration with the adaptive routing

of RPL. The TCP-based scheme offers the same protection as compared to other techniques such as IDS, rate limiting, or authentication but at a much lower level of resource consumption. We support it by a virtual analysis to indicate that connectivity remains even when power is switched off, and experimentally measure the parameters sensitivity. This is done by the 20 noes testbed and since this approach is completely distributed it is most likely to have a good scaling to larger deployments.

REFERENCES

[1] D. Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proc. 1st IEEE Int. Workshop on Sensor Network Protocols and Applications, 2003, pp. 113–127.

[3] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2–23, 2006.

[4] S. S. Buttyan, L. Buttyan, and I. Vajda, "Security of wireless sensor networks: A survey," IEEE Security & Privacy, vol. 11, no. 1, pp. 22– 31, Jan. 2013.

[5] M. A. S. Kamal, M. M. Akbar, M. M. Rahman, and M. Z. Islam, "A Study of Flooding Attacks in Wireless Sensor Networks," in Proc. Int. Conf. on Computer and Information Technology (ICCIT), 2007, pp. 1–5.

[6] D. E. Kouicem, H. Haffaf, and M. Bouhorma, "A survey of DoS attacks in Wireless Sensor Networks," in Proc. Int. Conf. on Multimedia Computing and Systems (ICMCS), 2014, pp. 1–6.

[7] P. Tague, M. Li, and R. Poovendran, "Mitigation of packet dropping attacks in wireless ad hoc networks," in Proc. Int. Conf. on Dependable Systems and Networks (DSN), 2006, pp. 1–10.

[8] E. J. Kim, F. J. Garcia, J. U. Kim, and J. C. S. Santos, "A survey on congestion control protocols in wireless sensor networks," Wireless Personal Communications, vol. 77, no. 3, pp. 1827-1854, 2014.

[9] S. G. Sanjay, S. S. Shashi, "Transmission Power Control in Wireless Sensor Networks: A Survey," IETE Technical Review, vol. 27, no. 3, pp. 225–231, 2010.

[10] M. C. Vuran and I. F. A. Akyildiz, "XLP: A cross-layer protocol for efficient communication in wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 9, no. 11, pp. 1578–1591, Nov. 2010.

[11] A. A. Ahmed, N. Fisal, J. A. Al-Dhief, and K. A. Al-Nabhani, "A Survey of Transmission Power Control based on Cross-Layer Design in Wireless Sensor Networks," in Proc. IEEE Conf. on Open Systems (ICOS), 2016, pp. 83–88.

[12] T. Winter, et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, Mar. 2012.

[13] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors," in Proc. 29th Annual IEEE Int. Conf. on Local Computer Networks, 2004, pp. 455– 462.

[14] N. A. K. S. Khan, M. H. Habaebi, and M. R. Islam, "Performance analysis of RPL under flooding attack in 6LoWPAN," in Proc. IEEE Int. Conf. on Signal Processing and Communication (ICSC), 2013, pp. 446–451.

[15] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross- Level Sensor Network Simulation with Cooja," in Proc. 31st IEEE Conf. on Local Computer Networks (LCN), 2006, pp. 601–608.