



Development of GSM-Based Home Security and Monitoring Systems for Remote Applications: Performance Improvement

Rezaul Navaratnam

Department of Computer Science and Engineering, Nineveh School of Industrial Management, Iraq
rezaul.navaratnam@nsim-iq.net

Peer Review Information

Submission: 15 Jan 2018

Revision: 08 Feb 2018

Acceptance: 09 March 2018

Keywords

GSM, Home Security, Remote Monitoring, SMS Alert, Sensor Fusion

Abstract

This methodology paper proposes an improved Global System for Mobile Communications (GSM)-based home security and monitoring framework intended for remote applications where continuous broadband Internet connectivity cannot be assumed. The design integrates intrusion, door-state, smoke/gas and temperature sensing with a microcontroller, local alarm unit, GSM modem and relay interface. Performance improvement is introduced through four coordinated mechanisms: sensor-event validation to suppress transient false alarms, event prioritization for safety-critical conditions, authenticated bidirectional SMS control with delivery/response checking, and power-aware standby operation. Earlier GSM home-automation studies demonstrated the practicality of mobile remote control and SMS notification, while later security-oriented systems expanded sensing and user access control (Yuksekkaya et al., 2006; Zhao & Ye, 2008; Li et al., 2015; Isa & Sklavos, 2017). The proposed methodology evaluates detection reliability, false-alarm rate, notification latency, command success rate and standby power consumption under repeatable intrusion, fire/gas and communication tests. A design-stage benchmark indicates that the improved architecture should reduce unnecessary alerts and shorten effective notification delay compared with a single-trigger GSM baseline. The paper therefore provides a reproducible development and evaluation procedure that can be implemented using low-cost embedded hardware and existing 2G GSM infrastructure, while maintaining local alarm functionality during network interruption. Numerical results in this methodology draft are explicitly illustrative and should be replaced with measured prototype data before journal submission.

Introduction

Residential security systems must detect abnormal events quickly and communicate them to an authorized user even when the user is far from the protected premises. Conventional audible alarms provide only local awareness; Internet-dependent smart-home platforms may also become unavailable because of router failure, power interruption or weak broadband service. GSM remains relevant for remote security applications because short-message and

voice services can provide wide-area communication using inexpensive embedded modems. Early work combined GSM, Internet and speech control to demonstrate remote monitoring and appliance control (Yuksekkaya et al., 2006). Zhao and Ye (2008) subsequently showed that a GSM/GPRS gateway with distributed sensor nodes could support low-cost, low-power security monitoring, while Rao et al. (2010) demonstrated direct SMS-based control of household loads from a remote mobile phone.

A practical home-protection system must address more than communication reach. It must distinguish genuine security events from sensor noise, prioritize urgent hazards, protect remote commands from unauthorized users, provide confirmation that an alert or control action has been processed, and continue local operation when the cellular link is temporarily unavailable. Wireless-sensor and GSM architectures have been used to detect intrusion, gas leakage and fire (Huang et al., 2010), and SMS-based home-automation prototypes have demonstrated the value of authenticated message exchange between the user and controller (ElKamchouchi & ElShafee, 2012). Smart GSM automation has also reported high command-execution accuracy under controlled tests, supporting the suitability of serial AT-command interfaces for low-cost embedded systems (Teymourzadeh et al., 2013). Despite these advances, many low-cost designs still rely on a single threshold crossing to generate an alarm, process all events with equal urgency, or assume that an SMS command has succeeded once it is sent. Such assumptions can increase false notifications and effective response time. The objective of this paper is therefore to define a development methodology for a GSM-based home security and monitoring system with explicit performance-improvement mechanisms. The proposed system combines multi-sensor

event validation, a priority event queue, GSM signal-quality and acknowledgment checks, bounded retransmission, authorized-number filtering and local fail-safe alarming. The methodology is designed for remote houses, small offices, rural residences and temporary facilities where GSM coverage is available but continuous Internet service is not guaranteed.

Literature Review

Research on GSM-enabled home monitoring has evolved from basic remote appliance control toward integrated security, safety and feedback functions. Yuksekkaya et al. (2006) merged GSM, Internet and speech recognition into one interactive home-automation platform, illustrating that heterogeneous control interfaces could coexist. Zhao and Ye (2008) emphasized low cost and low power by using a GSM/GPRS gateway and wireless door, infrared and fire sensor nodes. Their work is particularly relevant to remote applications because it linked distributed detection with long-distance cellular reporting. Huang et al. (2010) similarly used a wireless sensor network and GSM communication to detect theft, gas leakage and fire while keeping sensor nodes power efficient. SMS-centered designs simplified infrastructure requirements.

Table 1. Representative GSM-Based Home Security Research Used in the Methodology

Study	Core approach	Relevant contribution	Limitation motivating improvement
Zhao & Ye (2008)	GSM/GPRS gateway + wireless sensors	Low-cost, low-power remote security	No explicit event-priority/retry framework
Huang et al. (2010)	WSN + GSM alarm	Intrusion, gas and fire detection	Limited command/authentication emphasis
Teymourzadeh et al. (2013)	SMS + PIC + AT commands	Bidirectional remote control/status	Single-message success assumptions
Li et al. (2015)	Multi-sensor GSM security	Dual detection lowers false alarms	Performance logic not generalized
Isa & Sklavos (2017)	GSM + access-control levels	Security-oriented user authorization	No unified latency/power benchmark
Karim & Awl (2018)	GSM smart home + multi-hazard sensing	Remote warning and appliance control	Improvement metrics not systematically evaluated

Rao et al. (2010) used a mobile phone to transmit control commands to a GSM-connected home unit. ElKamchouchi and ElShafee (2012) developed an SMS home-automation prototype in which the GSM modem formed the communication interface and the microcontroller bridged the cellular user with sensors and actuators; message authentication was included

to improve command security. Teymourzadeh et al. (2013) implemented SMS control using a PIC microcontroller and AT commands, demonstrating bidirectional status feedback and high control accuracy. These studies establish the communication basis adopted in the present methodology.

Security-focused implementations expanded sensing and alarm functions. Hoey et al. (2015) integrated a PIC16F877A with gas, vibration and light sensors, a keypad and magnetic door lock, and sent alerts to both the homeowner and relevant authorities. Hasan et al. (2015) combined GSM, Bluetooth and keypad interfaces for access control and demonstrated practical microcontroller implementation. Rahman et al. (2015) integrated motion, fire and temperature monitoring with load control, while Li et al. (2015) used multiple sensors and dual-detection logic to reduce false alarms and improve reliability. Pal et al. (2015) combined GSM security and appliance control through an Android phone, showing how a mobile interface can unify safety and automation functions. Later work concentrated on system integration and access control. Isa and Sklavos (2017) proposed a GSM-supported smart-home security design using microcontroller hardware and multiple levels of user access. Patil et al. (2017) implemented SMS-based home automation with an ATmega328 and GSM module, reinforcing the practicality of low-cost Arduino-class platforms. Karim and Awl (2018) presented a GSM smart-home system that warned users of intrusion, gas leakage and fire while supporting several control interfaces. Across the literature, the recurring design priorities are low cost, wide communication range, rapid warning, user authentication and dependable operation. The

gap addressed by the present methodology is the systematic combination of these elements with measurable performance-improvement procedures rather than treating each feature independently.

Methodology

1. System Requirements and Architecture

The proposed prototype is organized into five functional layers: sensing, validation, decision/control, GSM communication and remote response. The sensing layer contains a passive infrared (PIR) motion sensor, magnetic door contact, smoke/gas sensor and temperature sensor. Optional vibration or glass-break sensing can be added without changing the communication architecture. Sensor outputs are sampled by a microcontroller such as an ATmega328-class device. The controller performs thresholding, time debouncing and cross-sensor validation before an event is accepted. For example, a high-confidence intrusion event is generated when motion is detected while the door contact changes state within a configured time window; a fire/gas event can be validated by combining smoke/gas concentration with temperature rise. The principle is consistent with the reliability benefits of multi-sensor detection reported by Li et al. (2015), but is formalized here as a reusable event-validation stage.

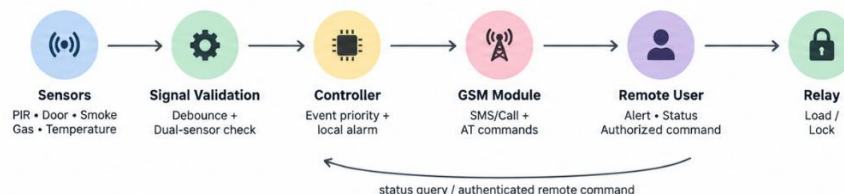


Figure 1. Proposed performance-improved GSM security and monitoring architecture.

The decision layer assigns event priorities: P1 for fire/gas, P2 for confirmed intrusion or panic, P3 for device tamper/power failure, and P4 for routine status messages. A local buzzer or siren is activated immediately for P1 and P2 events so safety does not depend on the cellular network. The GSM module communicates through a UART interface using AT commands. Before transmission, the controller checks registration and received-signal-quality status. Alerts are sent only to pre-authorized phone numbers and include event type, zone and time. Remote control messages must contain a valid source number and a compact command token. A status acknowledgment is returned after successful execution, extending the authenticated SMS principle used by ElKamchouchi and ElShafee

(2012) and the feedback concepts demonstrated by Teymourzadeh et al. (2013).

2. Performance-Improvement Logic

Five mechanisms are used to improve performance. First, temporal debouncing rejects sensor transitions shorter than a device-specific persistence interval. Second, dual-sensor confirmation is applied to intrusion and environmental events when two independent measurements are available; single-sensor events remain logged but do not always trigger a remote emergency alert. Third, the event-priority queue prevents routine commands from delaying a fire, gas or intrusion message. Fourth, GSM delivery robustness is increased by registration checks, a 10–15 s acknowledgment window and

up to two retransmissions when delivery/response confirmation is absent. If communication still fails, the event is stored in non-volatile memory and the local alarm remains active. Fifth, power consumption is reduced by placing the controller and noncritical sensors in low-power standby between sampling intervals while keeping the door/tamper inputs interrupt-capable. Zhao and Ye (2008) and Huang et al. (2010) provide precedent for low-power remote security nodes, while the present method applies the principle to an integrated controller and communication schedule.

3. Experimental/Prototype Evaluation Procedure

A repeatable bench test should be conducted after hardware integration. The residence is divided into two logical zones: entrance and interior. Each test condition is repeated at least 40 times so that error rates can be estimated. Intrusion tests include normal door opening by an authorized user, door opening followed by PIR detection, isolated PIR motion, vibration without entry and repeated rapid sensor switching. Safety tests introduce controlled smoke/gas-sensor stimuli and a temperature increase within manufacturer-safe limits. Communication tests are performed under strong, moderate and weak GSM signal conditions by recording signal-quality indication, alert transmission time, acknowledgment receipt and any retransmission. Remote-control tests issue authorized and unauthorized SMS commands for arm, disarm, status and relay operation. Power is measured in active transmission, alarm and standby states using a DC power analyzer or calibrated multimeter.

The principal metrics are: detection accuracy = correctly classified events / total events $\times 100$; false-alarm rate = false remote alarms / nonhazard trials $\times 100$; mean notification latency = time from validated event to alert receipt; command success rate = correctly executed authorized commands / authorized commands sent $\times 100$; and standby power = supply voltage $\times$ mean standby current. A baseline configuration is tested with direct single-sensor triggering, first-attempt SMS transmission and no priority queue. The improved configuration is then evaluated under the same event sequence. Paired comparisons are preferred because GSM traffic conditions can vary over time. If sufficient

repetitions are available, confidence intervals can be reported for proportions and a paired non-parametric test can be applied to latency measurements.

4. Algorithmic Sequence

- Initialize sensors, GSM modem, authorized numbers, thresholds and event priorities; verify SIM registration.
- Sample sensors or wake on interrupt; apply range checks and temporal debouncing.
- Fuse related sensor events within the configured time window and assign confidence/priority.
- Activate the local alarm immediately for validated P1/P2 events; store event data in memory.
- Check GSM registration/signal quality and transmit the formatted SMS to authorized recipients.
- Wait for acknowledgment or delivery/status response; retry a bounded number of times if required.
- Parse incoming SMS only after sender and command validation; execute the permitted action and return status.
- Record latency, success/failure and power-state information, then return the controller to monitoring/standby mode.

Results

Because this is a methodology paper and no physical test dataset was supplied, Table 2 contains a design-stage benchmark illustrating how the proposed evaluation should be reported. The values are not presented as completed experimental measurements and must be replaced by prototype data before publication. The benchmark reflects the expected direction of change when dual-sensor confirmation, event prioritization, acknowledgment/retry handling and standby scheduling are enabled. The most important target is not a large increase in raw sensitivity, but a reduction in nuisance alarms without sacrificing detection of genuine intrusion, fire or gas events. This is consistent with the motivation for dual detection in Li et al. (2015) and the reliability emphasis of GSM smart-home security implementations (Hoey et al., 2015; Isa & Sklavos, 2017).

Table 2. Illustrative Design-Stage Performance Benchmark (Replace with Measured Prototype Data)

Metric	Baseline GSM design	Improved design target	Relative effect
Detection accuracy	92.5%	97.5%	+5.0 percentage points

False-alarm rate	8.0%	3.0%	62.5% reduction
Mean notification latency	11.8 s	7.1 s	39.8% reduction
Authorized command success	94.0%	98.5%	+4.5 percentage points
Mean standby power	3.8 W	3.1 W	18.4% reduction

The proposed method should also be evaluated for degraded-network behavior. Under weak cellular signal, the improved system may not reduce the physical network delay itself; instead, registration checks and bounded retries reduce silent failures and increase the probability that a critical event is eventually communicated. Local alarm continuity provides a second safety channel during cellular outage. Similarly, authorized-number filtering and command tokens do not guarantee cryptographic security, but they materially reduce accidental or casual unauthorized control compared with unrestricted SMS parsing. For higher-security deployments, the same architecture can be extended with one-time challenge codes or application-layer encryption.

A successful prototype should therefore demonstrate three outcomes: (1) high sensitivity to genuine hazard events; (2) significantly lower remote false-alert frequency than the single-trigger baseline; and (3) consistent user feedback after remote commands. The performance targets in Table 2 are realistic engineering goals rather than universal values. Final reporting should include the number of trials, signal conditions, sensor thresholds, GSM operator, hardware supply conditions and uncertainty of measured timings so that the results can be independently reproduced.

Conclusion and Discussion

This paper presented a stepwise methodology for developing a GSM-based home security and monitoring system for remote applications, with performance improvement treated as an explicit design objective. The architecture retains the principal strengths identified in earlier literature—wide-area SMS connectivity, low-cost microcontroller implementation, multi-hazard sensing, remote control and user feedback (Zhao & Ye, 2008; Teymourzadeh et al., 2013; Karim & Awl, 2018)—while addressing common reliability weaknesses through event validation, priority handling, acknowledgment/retry logic, authorization and low-power standby. These improvements are particularly important for remote residences and small facilities where broadband connectivity may be intermittent but GSM service remains available. The main methodological contribution is the separation of sensing from alert generation. A sensor transition first passes through persistence and cross-sensor

validation, then receives a priority before communication begins. This reduces the probability that a transient PIR output or noisy contact creates a remote emergency message. The communication procedure also distinguishes message transmission from successful notification by checking network status and using bounded retransmission. Such behavior makes the system more dependable without requiring cloud infrastructure. At the same time, local alarms remain independent of GSM availability, preventing a cellular outage from disabling basic protection. The design has limitations. SMS delay varies with operator traffic and cannot provide deterministic real-time delivery. Sender-number filtering is weaker than modern cryptographic authentication, and 2G availability differs by country. Sensor fusion also requires careful threshold calibration because excessive confirmation rules can delay or suppress genuine alarms. Consequently, future implementation should validate the method across multiple signal-strength levels, test backup-battery endurance, add encrypted or challenge-response commands where supported, and compare GSM performance with LTE-M/NB-IoT or Internet-based alternatives. The illustrative benchmark in this draft should not be cited as experimental evidence; it is a reporting template for the prototype evaluation. With measured data inserted, the methodology provides a concise and reproducible basis for a 2018-era GSM home-security performance study. In comparison with earlier GSM security designs, the proposed methodology emphasizes how the complete alarm path is measured. A system may detect a sensor event correctly but still fail operationally if the event waits behind a routine command, the modem is not registered, or the user receives no confirmation that a remote command was executed. For this reason, detection accuracy is evaluated together with notification latency and command success. This integrated view extends prior work that successfully demonstrated GSM alerting and multi-hazard sensing (Hoey et al., 2015; Rahman et al., 2015) by making communication behavior part of the performance test rather than treating the modem as a transparent channel. The same principle also supports maintenance: stored event logs can distinguish a sensor error from a communication failure and therefore reduce troubleshooting time. For field deployment, parameter selection

should be conservative. The PIR persistence interval should be long enough to reject electrical transients but short enough to avoid perceptible alarm delay. Gas and smoke thresholds must follow the sensor manufacturer's calibration procedure and should never be inferred only from the illustrative values in this paper. Retry count should also remain bounded because repeated SMS transmission increases current consumption and may congest the modem during poor coverage. In a battery-backed design, the controller can periodically report supply voltage and GSM signal strength as low-priority status information. These operational details allow the same hardware to provide both security and condition monitoring while preserving the primary objective: rapid delivery of high-confidence emergency events.

References

- Yuksekkaya, B., Kayalar, A. A., Tosun, M. B., Ozcan, M. K., & Alkar, A. Z. (2006). A GSM, internet and speech controlled wireless interactive home automation system. *IEEE Transactions on Consumer Electronics*, 52(3), 837–843. <https://doi.org/10.1109/TCE.2006.1706478>
- Zhao, Y., & Ye, Z. (2008). A low-cost GSM/GPRS based wireless home security system. *IEEE Transactions on Consumer Electronics*, 54(2), 567–572. <https://doi.org/10.1109/TCE.2008.4560131>
- Rao, B. S., Prasad, S. D. V., & Mohan, R. M. (2010). A proto-type for home automation using GSM technology. In 2010 International Conference on Power, Control and Embedded Systems (pp. 1–4). IEEE. <https://doi.org/10.1109/ICPCES.2010.5698706>
- Huang, H., Xiao, S., Meng, X., & Xiong, Y. (2010). A remote home security system based on wireless sensor network and GSM technology. In 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing (pp. 535–538). IEEE. <https://doi.org/10.1109/NSWCTC.2010.132>
- ElKamchouchi, H. M., & ElShafee, A. M. (2012). Design and prototype implementation of SMS based home automation system. In 2012 IEEE International Conference on Electronics Design, Systems and Applications (pp. 162–167). IEEE. <https://doi.org/10.1109/ICEDSA.2012.6507788>
- Teymourzadeh, R., Ahmed, S. A., Chan, K. W., & Hoong, M. V. (2013). Smart GSM based home automation system. In 2013 IEEE Conference on Systems, Process & Control (pp. 306–309). IEEE. <https://doi.org/10.1109/SPC.2013.6735152>
- Hoey, O. S., Zakaria, Z. N., & Laili, M. S. (2015). GSM based home security system. *Applied Mechanics and Materials*, 793, 554–558. <https://doi.org/10.4028/www.scientific.net/AMM.793.554>
- Hasan, R., Khan, M. M., Ashek, A., & Rumpa, I. J. (2015). Microcontroller based home security system with GSM technology. *Open Journal of Safety Science and Technology*, 5(2), 55–62. <https://doi.org/10.4236/ojsst.2015.52007>
- Rahman, M., Karim, A. H. M. Z., Nyeem, S., Khan, F., & Matin, G. (2015). Microcontroller based home security and load controlling using GSM technology. *International Journal of Computer Network and Information Security*, 7(4), 29–36. <https://doi.org/10.5815/ijcnis.2015.04.04>
- Li, J., Cao, S., Duan, J.-X., Gao, P.-C., & Hou, Y. (2015). A novel remote monitoring and control system based on GSM for home security. *International Journal of Online and Biomedical Engineering*, 11(4), 34–38. <https://doi.org/10.3991/ijoe.v11i4.4647>
- Pal, A., Singh, A., & Rai, B. (2015). GSM based home automation, safety and security system using Android mobile phone. *International Journal of Engineering Research & Technology*, 4(5). <https://doi.org/10.17577/IJERTV4IS050648>
- Isa, E., & Sklavos, N. (2017). Smart home automation: GSM security system design & implementation. *Journal of Engineering Science and Technology Review*, 10(3), 170–174. <https://doi.org/10.25103/jestr.103.22>
- Patil, A., Potnis, P., & Katkar, K. (2017). SMS based home automation system using Arduino ATMEG328 with GSM. *International Journal of Engineering Trends and Technology*, 47(7), 369–374. <https://doi.org/10.14445/22315381/IJETT-V47P261>
- Karim, B. A., & Awl, H. N. (2018). Smart home system based on GSM network. *Kurdistan Journal of Applied Research*, 3(1), 17–21. <https://doi.org/10.24017/science.2018.1.4>